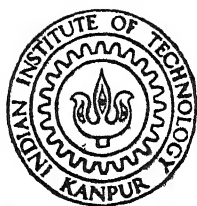


# ON OPTIMUM CODES AND THEIR COVERING RADII

*by*

MADHU SUDAN GARG



DEPARTMENT OF MATHEMATICS

INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

November, 1990

MATH  
990  
D  
GARG  
ON

# ON OPTIMUM CODES AND THEIR COVERING RADII

*A Thesis Submitted*  
in Partial Fulfilment of the Requirements  
for the Degree of  
DOCTOR OF PHILOSOPHY

*by*  
MADHU SUDAN GARG

*to the*  
DEPARTMENT OF MATHEMATICS  
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR  
November, 1990

## CERTIFICATE

It is certified that the work contained in the thesis entitled ''ON OPTIMUM CODES AND THEIR COVERING RADII'' by Mr. Madhu Sudan Garg, has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.



(M.C. BHANDARI)  
Thesis Supervisor  
Department of Mathematics  
Indian Institute of Technology  
Kanpur 208016, U.P.  
India

November, 1990

DEDICATED TO MY PARENTS

Shri Prem Chand Garg

Smt. Sarojini Garg



1972

72

CENTRAL LIBRARY  
UNIVERSITY OF KANSAS

NO. 7114034

MATH-1990-D-GAR-OPT

## ACKNOWLEDGEMENTS

I am indebted to my thesis supervisor Dr. M.C. Bhandari for having bestowed upon me his valuable guidance and inspiration at all stages of this research. My discussions with him were enlightening.

I have no word to express my gratitude for the affection showered on me by Dr.B.L. Dhooper and Shri Ramashish (social workers).

I am grateful to all my friends who have made this period of study a pleasant and memorable one.

Finally I express my thanks to Mr. Ashok Kumar Bhatia for typing this thesis.

Madhu Sudan Garg

| CONTENTS   | Page |
|--|------|
| NOMENCLATURE   | vii  |
| SYNOPSIS   | xi   |
| CHAPTER  |      |
| I. INTRODUCTION  | 1    |
| II. PRELIMINARIES AND SURVEY   | 5    |
| II.A. Optimum Codes  | 10   |
| II.B. Residual Code  | 16   |
| II.C. The Covering Radius Problem  | 19   |
| II.D. Normality of Codes   | 23   |
| II.E. The Number $\max_s(r, q)$  | 24   |
| III. COVERING RADIUS OF OPTIMUM CODES                                      | 27   |
| III.A. A Lower Bound   | 27   |
| III.B. An Upper Bound  | 28   |
| III.B.1. Applications  | 31   |
| III.B.2. An Upper Bound on $b(k, d)$                                       | 33   |
| III.B.3. Performance   | 35   |
| III.C. The Number $\max_s(r, q)$ And Its<br>Relation With Other Parameters | 36   |
| III.D. Bounds on $R(S_k(q))$   | 41   |
| III.D.1. Upper Bounds on $R(S_k(q))$                                       | 41   |
| III.D.2. Lower Bound on $R(S_k(q))$  | 43   |
| III.D.3. Bounds on $R(S_k(q))$ for<br>$q = 3, 4$ and $5$                   | 45   |

|       |   |    |
|-------|---|----|
| IV.   | MINIMAL LENGTH OF 9-DIMENSIONAL BINARY                |    |
|       | LINEAR CODES  | 46 |
| IV.A. | $n(9,d)$ for $d > 256$                                | 46 |
| IV.B. | Known Bounds on $n(9,d)$ for $d \leq 256$             | 55 |
| IV.C. | Upper Bounds on $n(9,d)$ for Certain<br>Values of $d$ | 58 |
| IV.D. | Nonexistence of Certain Codes                         | 61 |
| V.    | OPTIMUM CODES OF DIMENSION 3 AND 4 OVER               |    |
|       | $GF(4)$   | 73 |
| V.A.  | General Results                                       | 73 |
| V.B.  | Determination of $n_4(3,d)$                           | 74 |
| V.C.  | Bounds on $n_4(4,d)$                                  | 76 |
| V.D.  | Some Improvements in Table 5.1                        | 79 |
|       | REFERENCES  | 82 |

## NOMENCLATURE

|            |   |
|------------|---|
| $q$        | $\equiv p^m$ , where $p$ is a prime and $m$ is a positive integer, p.1.                           |
| $GF(q)$    | Galois field with $q$ elements, p.1.  |
| $[n,k,d]$  | Length, dimension and minimum distance of a linear code over $GF(q)$ , p.1.                       |
| $C$        | An $[n,k,d]$ code, p.1.   |
| $R(C)$     | Covering radius of the code $C$ , p.1.  |
| $[x]$      | The smallest integer greater than or equal to $x$ , p.1.  |
| $g_q(k,d)$ | $\equiv \sum_{i=0}^{k-1} [d/q^i]$ , p.1.  |
| $n_q(k,d)$ | The minimal length of a linear code over $GF(q)$ of dimension $k$ and minimum distance $d$ , p.1. |
| $[n,k]$    | Length and dimension of a linear code over $GF(q)$ , p.3.   |
| $d_q[n,k]$ | The maximal minimum distance of an $[n,k]$ code, p.3.   |
| $k_q[n,d]$ | The maximal dimension of a linear code over $GF(q)$ of length $n$ and minimum distance $d$ , p.3. |
| $GF(q)^n$  | The set of all $n$ -tuples over $GF(q)$ , p.5.  |
| $wt(x)$    | Weight of a vector $x$ , p.5.   |

|                   |  |
|-------------------|--|
| $d(x,y)$          | Distance between the vectors $x$ and $y$ , p.5.                                  |
| $d(x,s)$          | Distance of a vector $x$ from a set $S$ , p.5.                                   |
| $H_k(q)$          | Hamming code of dimension $k$ over $GF(q)$ , p.6.                                |
| $S_k(q)$          | Simplex code of dimension $k$ over $GF(q)$ , p.6.                                |
| $G_k(q)$          | A generator matrix for $S_k(q)$ , p.6.   |
| $S_k$             | Binary Simplex code of dimension $k$ , p.6.                                      |
| $[A B]$           | Juxtaposition of matrices $A$ and $B$ , p.7.                                     |
| $[M \setminus A]$ | Matrix obtained by deleting columns of the matrix $A$ from the matrix $M$ , p.7. |
| $C_{k;u}(q)$      | The MacDonald code of dimension $k$ over $GF(q)$ , $1 \leq u \leq k-1$ , p.7.    |
| $RM(1,k-1)$       | First order binary Reed-Muller code of dimension $k$ , p.7.                      |
| $C^\perp$         | Dual of a code $C$ .   |
| $A_i$             | Number of codewords of weight $i$ in a code $C$ , p.8.                           |
| $B_i$             | Number of codewords of weight $i$ in $C^\perp$ , p.8.                            |
| $g(k,d)$          | $\equiv g_2(k,d)$ , p.9.   |
| $n(k,d)$          | $\equiv n_2(k,d)$ , p.9.   |
| $Res(C,c)$        | Residual code of $C$ with respect to the codeword $c \in C$ , p.16.              |
| $Res(C,w)$        | Residual code of $C$ with respect to the number $w$ , p.16.                      |

|                                       |  |
|---------------------------------------|--|
| $\lfloor x \rfloor$                   | The largest integer less than or equal to $x$ , p.17.  |
| $x^{tr}$                              | Transpose of a vector $x$ , p.23.  |
| $C_{\alpha}^{(i)}$                    | The set of codewords of a code $C$ , whose $i$ th coordinate is $\alpha$ , p.24.   |
| $H(C) = H_q(n, k, d)$                 | $\equiv n - g_q(k, d) + d - \lceil d/q^k \rceil$ , p.24.   |
| $(n, s)$ -set in $GF(q)^T$            | A set having $n, r$ -tuples over $GF(q)$ such that any $s$ of them are linearly independent, p.24.   |
| $\max_s(r, q)$                        | The maximal value of $n$ for which an $(n, s)$ -set in $GF(q)^T$ exists, p.24.   |
| $t[n, k]$                             | The minimal covering radius of a binary $[n, k]$ code, p.27.   |
| $b_q(k, d)$                           | $\equiv n_q(k+1, d) - n_q(k, d)$ , p.29.   |
| $b(k, d)$                             | $\equiv n(k+1, d) - n(k, d)$ , p.29.   |
| $t_k(q)$                              | The maximum number of $(-1)$ 's in any vector of $S_k(q)$ , p.43.  |
| $wt(a+C)$                             | $= d(a, C)$ , p.44.  |
| $\mathcal{C}_f(u_1, u_2, \dots, u_p)$ | The set of all $k \times n'$ , $n' = \sum_{i=1}^p (2^{u_i} - 1)$ matrices $G'$ for which the distance between any two vectors of $C'$ (generated by $G'$ ) is at most $\sum_{i=1}^p 2^{u_i - 1}$ , p.50. |

$\hat{U}(k,u)$ 

Set of all  $u$ -dimensional subspaces of  $GF(2)^k$ , p.50.

 $U(k,u)$ 

$\equiv \{\hat{U} \setminus \{0\} : \hat{U} \in \hat{U}(k,u)\}$  , p.50.

 $a|b$ 

$a$  divides  $b$



SYNOPSIS  
OF THE  
Ph. D DISSERTATION

ON OPTIMUM CODES AND THEIR COVERING RADII

BY

Madhu Sudan Garg  
Department of Mathematics, Indian Institute of Technology,  
Kanpur-208016 (India)

A linear code  $C$  of length  $n$ , dimension  $k$  and minimum distance  $d$ , over the Galois field  $GF(q)$  is called an  $[n, k, d]$  code. If  $q = 2$  then the code is called a binary code. In 1965 Solomon and Stiffler [8] proved that for given  $k$  and  $d$ , the minimum value of  $n$  (denoted by  $n_q(k, d)$ ) satisfies

$$n_q(k, d) \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \equiv g_q(k, d),$$

where  $\lceil x \rceil$  denotes the smallest integer  $\geq x$ . However the particular case  $q = 2$  was first proved by Griesmer [5].

An  $[n_q(k, d), k, d]$  code is called an optimum code and a  $[g_q(k, d), k, d]$  code, if it exists is called a Griesmer code. For simplicity one usually writes  $n(k, d)$  and  $g(k, d)$  for  $n_2(k, d)$  and  $g_2(k, d)$  respectively.

Determining  $n_q(k, d)$  for given  $k, d$  and  $q$  is a difficult task. In recent years many researchers like Baumert and McEliece [1], van Tilborg [10], Dodunekov and Manev [4] and

many others have tried to find  $n(k,d)$  for  $k \leq 8$ . For  $q > 2$  little is known about  $n_q(k,d)$ .

Another parameter of basic importance for a code is its covering radius, i.e., the weight of a maximum weight coset leader. Determining covering radius  $R(C)$  for a given code  $C$  is another difficult task. A number of lower and upper bounds on  $R(C)$  have been obtained by many researchers. For a survey of known results on the covering radius reader is referred to [2],

The present dissertation aims at determining (1) lower and upper bounds on the covering radius of an optimum code that are better than the other known bounds restricted to optimum codes (2) bounds on  $n(9,d)$  and  $n_4(k,d)$ ;  $k = 3,4$ . As an application of (1) bounds on the covering radius of a Simplex code over  $GF(q)$  (an open problem posed by Janwa [6]) and exact covering radius of many optimum codes, like MacDonald codes are obtained.

The covering radius of a binary Griesmer code  $C$  satisfies the inequality

$$R(C) \geq g(k,d) - 2^{k-1}.$$

Examples of binary Griesmer codes for which the above bound is better than the best lower bound  $t[n,k]$  (= the minimum covering radius of any binary  $[n,k]$  code) [2]; are given.

For given  $k,d$  and  $q$ , let the number ' $n_q(k+1,d) - n_q(k,d)$ ' be denoted by  $b_q(k,d)$ . Obviously  $b_q(k,d) \geq 1$ . However if

$k \geq 2$  and  $d \geq 5$  then it is shown that  $b_2(k,d) \leq \lceil \frac{d}{2} \rceil - 1$ . The following three results are proved.

**Theorem 1** : The covering radius of any  $[n,k,d]$  code  $C$  with  $n < n_q(k+1,d)$  satisfies  $R(C) \leq d - (n_q(k+1,d) - n)$ .

**Theorem 2** : The covering radius of an optimum code  $C$  satisfies  $R(C) \leq d - b_q(k,d)$ .

**Theorem 3** : An  $[n_q(k,d),k,d]$  code has covering radius  $d - b_q(k,d)$  if and only if there exists an  $[n_q(k+1,d),k+1,d]$  code with  $b_q(k,d)$  equivalent coordinates.

The importance of Theorem 2 is demonstrated by using it to (1) determine exact covering radius of many optimum codes and (2) show that the optimum codes with covering radius  $d-1$  are normal.

In [7] Janwa has shown that for an optimum code  $C$ ,  $R(C) \leq d - \lceil d/q^k \rceil$ . The following theorem shows that the bound given by Theorem 2 is better than this bound.

**Theorem 4** : If  $n_q(k,d) = g_q(k,d)$  or  $d \leq q^k$  then  $d - b_q(k,d) \leq d - \lceil d/q^k \rceil$ . However if  $n_q(k,d) = g_q(k,d) + t$  and  $n_q(k+1,d) = g_q(k+1,d) + t_1$ ,  $0 \leq t < t_1$ ; then  $d - b_q(k,d) < d - \lceil d/q^k \rceil$ .

Let  $\max_s(r,q)$  denote the maximum number of  $r$ -tuples over  $GF(q)$  with any  $s$  of them being linearly independent. If  $C$  is an  $[n,n-r,d]$  code, then any  $d-1$  columns of any parity check matrix for  $C$  are linearly independent. Hence  $\max_{d-1}(r,q) \geq n$ . For  $n > r$  the converse is also true. Using this concept it

is shown that the bound given by Theorem 2 is the best possible for  $b_q(k,d) = 1$ . If  $k_q[n,d] = \max\{k: \text{there exists an } [n,k,d] \text{ code}\}$  then the following theorem explores relations among various parameters of a code.

**Theorem 5 :** Let  $n_q(k,d) = n$  and let  $n-k = r$ . Then the following are equivalent

- (i)  $\max_{d-1}(r,q) = n$ ,
- (ii)  $k_q[n,d] = k_q[n+1,d] = k$ ,
- (iii)  $b_q(k,d) \geq 2$ ,
- (iv) every  $[n,k,d]$  code has covering radius  $\leq d-2$ .

Let  $S_k(q)$  denotes the  $[(q^k-1)/(q-1), k, q^{k-1}]$  Simplex code over  $GF(q)$ . It is known that  $R(S_k(2)) = 2^{k-1}-1$ . If  $q > 2$ , then almost nothing is known about  $R(S_k(q))$ . In [6] Janwa has posed this as an open problem. Since  $S_k(q)$  is an optimum code, it is maximal [3] and hence  $R(S_k(q)) \leq q^{k-1}-1$  [2]. This bound can be further improved for certain values of  $k$  and  $q$ .

**Theorem 6 :** (i) If  $q$  is even then  $R(S_2(q)) = q-1$ .

(ii) If  $q$  is odd then  $R(S_2(q)) \leq q-2$ . This bound is shown to be attained for  $q = 3$  and  $5$ .

(iii)  $R(S_k(q)) \leq q^{k-1}-2$ , for  $k \geq 3$  and  $q = 3$  or  $4$ . The bound is attained for  $k = q = 3$ .

Let  $t_k(q)$  denotes the maximum number of  $(-1)$ 's in any vector of  $S_k(q)$ . A lower bound on  $R(S_k(q))$  is given by following two theorems.

**Theorem 7 :**  $R(S_k(q)) \geq n - t_k(q)$  and  $t_m(q) = q^{m-k} t_k(q)$  for  $m \geq k$ .

**Theorem 8 :** (i)  $R(S_k(3)) \geq \frac{2 \cdot 3^{k-1} - 3^{k-2} - 1}{2}$   
 (ii)  $R(S_k(4)) \geq \frac{3 \cdot 4^{k-1} - 2 \cdot 4^{k-2} - 1}{3}$   
 (iii)  $R(S_k(5)) \geq \frac{3 \cdot 5^{k-1} - 2 \cdot 5^{k-2} - 1}{4}$

Tilborg [9] has shown that if  $d > t2^{k-1}$ , where  $t = \lfloor (-3 + \sqrt{8k+1})/2 \rfloor$ , then  $n(k,d) = g(k,d)$ . This bound is further improved. Let  $s = \lfloor d/2^{k-1} \rfloor$  and let  $v_1, v_2, \dots, v_t$  be positive integers defined inductively as follows.

$v_1$  is the largest integer  $u < k$  for which  $\sum_{i=1}^{\min\{u-2, s+1\}} (u-i) \leq sk$ .  
 Suppose  $v_1, v_2, \dots, v_{j-1}$  are defined for some  $j < t$ . Choose  $v_j$  to be the largest integer  $u < v_{j-1}$  for which  $\sum_{i=1}^{\min\{u-2, s-j+2\}} (u-i) \leq sk - \sum_{i=1}^{j-1} v_i$ .  
 Finally let  $v_t = sk - \sum_{i=1}^{t-1} v_i$ .

**Theorem 9 :**  $n(k,d) = g(k,d)$  for  $d \geq (t-1)2^{k-1} - v$ , where  
 $v = 2^{v_1-1} + 2^{v_2-1} + \dots + 2^{v_{t-1}-1} + 2^{v_t-2} + \dots + 2$ .

In particular if  $k = 9$ , then the above theorem yields that  $n(9,d) = g(9,d)$  for  $d \geq 337$ . The equality is also shown to hold for  $257 \leq d \leq 322$  by constructing certain 9-dimensional binary Griesmer codes. However the case  $323 \leq d \leq 336$  remains unsolved.

A table of bounds on  $n(9,d)$  for  $d \leq 256$  is formed using known results. Bounds are further improved by constructing certain binary 9-dimensional codes and by showing nonexistence of certain binary linear codes. The results are summarized by following four theorems.

Theorem 10:  $n(9,66) \leq 145$ ,  $n(9,68) \leq 149$ ,  $n(9,70) \leq 153$ ,  
 $n(9,72) \leq 156$ ,  $n(9,80) \leq 172$ ,  $n(9,86) \leq 184$  and  $n(9,88) \leq 187$ .

Theorem 11: If  $3 \leq i \leq k-4$  and  $k \geq 9$  then  $n(k, 2^{k-i}) \geq g(k, 2^{k-i}) + 3$ .

Theorem 12: Binary  $[53, 9, 24]$ ,  $[101, 10, 48]$ ,  $[116, 9, 56]$ ,  $[125, 10, 60]$ ,  
 $[196, 9, 96]$ ,  $[228, 9, 112]$  and  $[354, 9, 176]$  codes do not exist .

Theorem 13: Let  $d = 2^{k-4} - 2^m$ ,  $k \geq 10$ ,  $m \geq 0$ . Then  
 $n(k, d) \geq g(k, d) + 3$ .

If  $q > 2$  then much less is known about  $n_q(k, d)$ . Dodunekov [3] has generalized some of the results on binary codes to codes over  $GF(q)$ . Using his results the following theorem is proved.

Theorem 14:  $n_4(3, d) = \begin{cases} g_4(3, d) & , \text{ if } d \neq 7, 8 \\ g_4(3, d) + 1 & , \text{ if } d = 7, 8 \end{cases}$  .

Let  $q = p^m$ ,  $m = ts$  and let  $n' = (p^m - 1)/(p^s - 1)$ . If  $\{\alpha_1, \alpha_2, \dots, \alpha_t\}$  is any basis for  $GF(p^m)$  over  $GF(p^s)$  and if  $\beta_1, \beta_2, \dots, \beta_t$  are the rows of a generator matrix for  $S_t(p^s)$ , then the linear mapping  $f$  from  $GF(p^m)$  into  $GF(p^s)^{n'}$  satisfying  $f(\alpha_i) = \beta_i$  is an isomorphism. Moreover if  $C$  is any  $[n, k, d]$  code over  $GF(p^m)$  then mapping each codeword  $(x_1, x_2, \dots, x_n)$  to  $(f(x_1), f(x_2), \dots, f(x_n))$  one gets an  $[n(p^m - 1)/(p^s - 1), tk, (p^s)^{t-1}d]$  code over  $GF(p^s)$ . This observation is used to prove the following results.

Theorem 15: If  $k \geq 4$  and  $d \in \{4^{k-2} - 1, 4^{k-2}, 2 \cdot 4^{k-2} - 5,$

$2 \cdot 4^{k-2}-4, 3 \cdot 4^{k-2}-5, 3 \cdot 4^{k-2}-4\}$  then  $n_4(k,d) > g_4(k,d)$ .

Theorem 16 : If  $d \in \{3,4,7,8,15,16,43,44\}$  or  $25 \leq d \leq 32$  then  $n_4(4,d) > g_4(4,d)$ .

Theorem 17 :  $n_4(4,d) = g_4(4,d)$  for  $45 \leq d \leq 64, 93 \leq d \leq 96, 105 \leq d \leq 128, 141 \leq d \leq 144, 157 \leq d \leq 160, 173 \leq d \leq 192, 201 \leq d \leq 208$  and  $d \geq 213$ .

Theorem 18 :  $n_4(4,4d) \leq 5g_{16}(2,d)$ .

### REFERENCES

- [1] L.D. Baumert and R.J. McEliece, 'A note on the Griesmer bound', IEEE Trans. Inform. Theory, Vol. IT-19, pp. 134-135, 1973.
- [2] G.D. Cohen, M.R. Karpovsky, H.F. Mattson Jr., and J.R. Schatz, 'Covering radius-Survey and recent results', IEEE Trans. Inform. Theory, Vol. IT-31, pp. 328-343, 1985.
- [3] S.M. Dodunekov, 'Minimal block length of a linear  $q$ -ary code with specified dimension and code distance', Prob. Inform. Transm., Vol. 20, pp. 239-249, 1984.
- [4] S.M. Dodunekov and N.L. Manev, 'An improvement of the Griesmer bound for some small minimum distances', Discrete Applied Mathematics, Vol. 12, pp. 103-114, 1985.
- [5] J.H. Griesmer, 'A bound for error-correcting codes', IBMJ. Res. Develop. Vol. 4, pp. 532-542, 1960.

- [6] H. Janwa, "'Some new upper bounds on the covering radius of binary linear codes'", IEEE Trans. Inform. Theory, Vol. IT-35, pp. 110-122, 1989.
- [7] H. Janwa, "'On the covering radius of  $q$ -ary codes'", to appear.
- [8] G. Solomon and J.J. Stiffler, "'Algebraically punctured cyclic codes'", Information and control, Vol.8, pp. 170-179, 1965.
- [9] H.C.A. van Tilborg, "'On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound'", Information and control, Vol. 44, pp. 16-35, 1980.
- [10] H.C.A. van Tilborg, "'The smallest length of binary 7-dimensional linear codes with prescribed minimum distance'", Discrete Mathematics, Vol. 33, pp. 197-207, 1981.



## CHAPTER I

### INTRODUCTION

An  $[n,k,d]$  code is a linear code over the Galois field  $GF(q)$  with  $q$  elements ( $q = p^m$ , for some prime  $p$  and for some positive integer  $m$ ) of length  $n$ , dimension  $k$  and minimum distance  $d$ . For given  $k$  and  $d$  the minimal value of  $n$  for which an  $[n,k,d]$  code exists is denoted by  $n_q(k,d)$  and an  $[n_q(k,d), k, d]$  code is called an optimum code. In 1965 Solomon and Stiffler [41] showed that

$$n_q(k,d) \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \equiv g_q(k,d).$$

However the particular case  $q = 2$  was first proved by Griesmer [22]. The bound  $g_q(k,d)$  is usually called the Griesmer bound and a  $[g_q(k,d), k, d]$  code, if it exists is called a Griesmer code.

Determining  $n_q(k,d)$  for given  $k,d$  and  $q$  is a difficult task. In recent years many researchers like Baumert and McEliece [2], van Tilborg [43], Dodunekov and Manev [16] and many others have tried to find  $n_2(k,d)$  for  $k \leq 8$ . For  $q > 2$  little is known about  $n_q(k,d)$  [12].

Another parameter of basic importance for a code is its covering radius, i.e., the weight of a maximum weight coset leader. Determining covering radius  $R(C)$  for a given code  $C$

is another difficult task. A number of lower and upper bounds on  $R(C)$  have been obtained by Cohen, Karpovsky, Mattson and Schatz [8], Delsarte [11], Helleseeth, Kløve and Mykkeltveit [25], Janwa [32] and by many others.

The present dissertation aims at determining (i) lower and upper bounds on the covering radius of an optimum code that are better than the other known bounds restricted to optimum codes (ii) bounds on  $n(9,d)$  and  $n_4(k,d)$  ;  $k = 3,4$ . As an application of (i) bounds on the covering radius of a Simplex code over  $GF(q)$  (an open problem posed by Janwa [32]) and exact covering radius of many optimum codes **are obtained**. The organization of the dissertation is as follows.

Chapter II contains some essential known results on properties of optimum codes, bounds on  $n_q(k,d)$ , residual of a code, covering radius and normality. Some easy consequences of the concept of a residual code like (i) determination of an upper bound on the minimum distance of certain cyclic codes and (ii) characterization of binary Simplex code and Reed-Muller code of first order are also derived.

Lower and upper bounds on the covering radius of an optimum code are obtained in Chapter III. The bounds are shown to be better than other known bounds restricted to optimum codes. Exact covering radius of a subcode of index  $q$  of an optimum code is found and used to give a sufficient

condition for the normality of optimum codes. Theorems giving relations among different parameters of a code like  $n_q(k,d)$ , covering radius,  $\max_s(r,q)$  (the maximum number of  $r$ -tuples over  $GF(q)$  such that any  $s$  of them are linearly independent),  $d_q[n,k]$  (the maximum minimum distance of any  $[n,k]$  code) and  $k_q[n,d]$  (the maximum dimension of any code of length  $n$  and minimum distance  $d$ ) are also established. Finally the results are used to determine bounds on the covering radius of a Simplex code over  $GF(q)$ . This was posed as an open problem by Janwa [32].

In 1980 Tilborg [42] proved that for a fixed  $k$  if  $d > \lceil (-3 + \sqrt{8k+1})/2 \rceil 2^{k-1}$  then  $n_2(k,d) = g_2(k,d)$ . This bound is improved in Chapter IV which in particular shows that  $n_2(9,d) = g_2(9,d)$  for  $d \geq 337$ . A table of bounds on  $n_2(9,d)$  for  $d \leq 256$ , using known results is also constructed. The bounds are further improved by showing nonexistence of certain codes of dimension 9 and by constructing certain 9-dimensional binary codes. Some general results on the lower bound for  $n_2(k,d)$  are also derived.

Chapter V is devoted to the problem of determining  $n_4(k,d)$  for  $k=3$  and  $\infty$ . Basic results of Dodunekov [12] on  $n_q(k,d)$  are used to determine  $n_4(3,d)$  and lower bounds on  $n_4(4,d)$ . An isomorphism between codes over  $GF(p^m)$  and codes over  $GF(p^s)$ ,

is a positive divisor of  $m$ , is established. This relation to show nonexistence of certain  $[g_4(k,d), k, d]$  codes over  $\mathbb{F}_4$  and for determining an upper bound for  $n_4(4,d)$ .

## CHAPTER II

### PRELIMINARIES AND SURVEY

A field is a nonempty set  $F$  with two binary operations denoted by '+' and '.' satisfying (i)  $(F,+)$  is an abelian group (ii) nonzero elements of  $F$  form an abelian group under '.' and (iii)  $a.(b+c) = a.b + a.c$  for all  $a,b,c \in F$ . If  $F$  has finite number of elements, then  $F$  is called a finite field. Galois has shown that a finite field with  $q$  elements exists if and only if  $q = p^m$ , for some prime  $p$  and for some positive integer  $m$ . Moreover a finite field with  $q$  elements is unique up to isomorphism and is usually denoted by  $GF(q)$ . For results on finite fields we refer to [38]. Let  $GF(q)^n$  denotes the set of all  $n$ -tuples over  $GF(q)$ . For  $x, y \in GF(q)^n$ , weight of  $x$  (denoted by  $wt(x)$ ) is the number of nonzero components in  $x$  and distance between  $x$  and  $y$  (denoted by  $d(x,y)$ ) is the weight of  $x-y$ . For a subset  $S$  of  $GF(q)^n$ , distance between  $x$  and  $S$  (denoted by  $d(x,S)$ ) is  $\min \{d(x,y): y \in S\}$ . If  $x = (x_1, x_2, \dots, x_n)$  and  $y = (y_1, y_2, \dots, y_n)$  then  $x_i$  is called the  $i$ th coordinate of  $x$  and the vector  $(x_1y_1, x_2y_2, \dots, x_ny_n)$  (denoted by  $x*y$ ) is called the intersection of  $x$  and  $y$ .

A linear code  $C$  of length  $n$  is a subspace of  $GF(q)^n$ . If  $C$  has dimension  $k$  and minimum distance  $d$  then it is called an  $[n,k,d]$  code. Elements of a code are called codewords and the phrase 'the  $i$ th coordinate of  $C$ ' means the  $i$ -th

coordinate function of  $C$ . If  $q = 2$  then the code is called a binary  $[n,k,d]$  code. Any  $[n,k]$  linear code  $C$ , being a subspace can be described either by giving a basis for it or by identifying an  $(n-k) \times n$  matrix  $H$  whose solution space is  $C$ . The matrix  $H$  is called a parity check matrix for  $C$ . A  $k \times n$  matrix whose rows form a basis for  $C$  is called a generator matrix for the  $[n,k]$  code  $C$ .

Let  $G_k(q)$  be the matrix whose columns consist of all nonzero  $k$ -tuples over  $GF(q)$  with any two columns linearly independent. Then the solution space of  $G_k(q)X = 0$  is a  $[(q^k-1)/(q-1), ((q^k-1)/(q-1))-k, 3]$  code (denoted by  $H_k(q)$ ).  $H_k(q)$  is called the Hamming code. On the other hand the code generated by the matrix  $G_k(q)$  is a  $[(q^k-1)/(q-1), k, q^{k-1}]$  code (denoted by  $S_k(q)$ ).  $S_k(q)$  is called the Simplex code. It is easy to see by induction that the matrix

$$G_{k+1}(q) = \left[ \begin{array}{c|c|c|c|c} 0 & 0 & \dots & 0 & 1 \\ & & & & 0 \\ & G_k(q) & & & \vdots \\ & & & G_k(q) & \vdots \\ & & & & 0 \end{array} \middle| \begin{array}{c|c|c|c} 1 & 1 & \dots & 1 \\ & & & \\ & & & \\ & & & \end{array} \middle| \begin{array}{c} \dots \\ \dots \\ \dots \end{array} \middle| \begin{array}{c} \alpha_{q-2} \alpha_{q-2} \dots \alpha_{q-2} \\ G_k(q) \end{array} \right]$$

is a generator matrix for  $S_{k+1}(q)$ , where  $GF(q) = \{0, 1, \alpha_1, \alpha_2, \dots, \alpha_{q-2}\}$

Moreover every nonzero codeword of  $S_{k+1}(q)$  has weight  $q^k$ .

The binary Simplex code of dimension  $k$  is denoted by  $S_k$ .

The code generated by the matrix

$$\left[ \begin{array}{c|c} 1 & 1 & \dots & 1 & 1 \\ \hline & G_k(2) & & & \begin{smallmatrix} 0 \\ \cdot \\ \cdot \\ 0 \end{smallmatrix} \end{array} \right]$$

is called the first order binary Reed-Muller code (denoted by  $\underline{RM}(1,k)$ ). Note that  $RM(1,k)$  is a  $[2^k, k+1, 2^{k-1}]$  code.

Let  $M$  be a matrix written as the juxtaposition of matrices  $A$  and  $B$ , that is  $M = [A|B]$ .  $A$  is denoted by  $[M \setminus B]$ . For  $1 \leq u \leq k-1$ , the code  $C_{k;u}(q)$  generated by the matrix

$$(2.1) \quad \left[ G_k(q) \setminus \frac{0}{G_u(q)} \right]$$

is called a MacDonald code [16]. Note that  $C_{k;u}(q)$  is a  $[(q^k - q^u)/(q-1), k, q^{k-1} - q^{u-1}]$  code [12]. We usually write  $C_{k;u}$  for  $C_{k;u}(2)$ .

Two codes are said to be equivalent if a generator matrix for one can be obtained from a generator matrix for the other by a column permutation followed by multiplying some columns by nonzero elements of  $GF(q)$ . Every  $[(q^k - q^u)/(q-1), k, q^{k-1} - q^{u-1}]$  code is equivalent to  $C_{k;u}(q)$  [12].

If  $x = (x_1, x_2, \dots, x_n)$ ,  $y = (y_1, y_2, \dots, y_n) \in GF(q)^n$  then  $x \cdot y = \sum_{i=1}^n x_i y_i \pmod{q}$  defines an inner product on

$GF(q)^n$ . If  $C$  is an  $[n,k]$  code then  $C^\perp = \{u \in GF(q)^n : u \cdot c = 0, \text{ for all } c \in C\}$ , called dual of  $C$ , is an  $[n,n-k]$  code.

Moreover a generator matrix for  $C$  is a parity check matrix for  $C^\perp$  and vice versa. Thus the Simplex code  $S_k(q)$  is the dual of the Hamming code  $H_k(q)$ . A code  $C$  is called self orthogonal or weakly self dual if  $C \subseteq C^\perp$ . If  $C = C^\perp$  then  $C$  is called self dual.

Let  $A_i$ ,  $0 \leq i \leq n$ ; denote the number of codewords of weight  $i$  in an  $[n,k,d]$  code  $C$ . Then  $\langle A_i \rangle$ ,  $0 \leq i \leq n$ ; is called the weight distribution of  $C$ . Obviously  $A_0 = 1$  and  $A_i = 0$  for  $1 \leq i \leq d-1$ . In 1963 MacWilliams determined a set of equations, usually called 'MacWilliams equations' relating the weight distribution of  $C^\perp$  to the weight distribution of  $C$  [38].

**Proposition 2.1** [38]. Let  $\langle A_i \rangle$  and  $\langle B_i \rangle$ ,  $0 \leq i \leq n$ ; be the weight distributions of a linear code  $C$  and its dual  $C^\perp$  respectively. Then

$$B_m = |C|^{-1} \sum_{i=0}^n A_i K_m(i), \quad 0 \leq m \leq n;$$

where  $K_m(x) = \sum_{j=0}^m (-1)^j \binom{n-x}{m-j} \binom{x}{j} = (-1)^m K_m(n-x)$ ,  $0 \leq m \leq n$ ;

$K_m(x)$  is called the Krawtchouk polynomial.

Determining  $K_m(x)$  is a laborious task. The help of a computer is taken to compute  $K_m(x)$  for certain values of  $m, n$  and  $x$ .



For given  $k$  and  $d$  the minimum value of  $n$  for which there exists an  $[n, k, d]$  code is denoted by  $n_q(k, d)$ . In 1965 Solomon and Stiffler [41] have shown that

$$(2.2) \quad n_q(k, d) \geq \sum_{i=0}^{k-1} [d/q^i] \equiv g_q(k, d),$$

where  $[x]$  denotes the least integer  $\geq x$ . However the particular case  $q = 2$  was first proved in 1960 by Griesmer [22]. For simplicity one usually writes  $n(k, d)$  and  $g(k, d)$  for  $n_2(k, d)$  and  $g_2(k, d)$  respectively. The lower bound on  $n_q(k, d)$  given by (2.2) is usually called the Griesmer bound and the code  $[g_q(k, d), k, d]$ , if it exists is called a code meeting the Griesmer bound or simply a Griesmer code. It is easy to verify that Hamming, Simplex and MacDonald codes are examples of Griesmer codes. An  $[n_q(k, d), k, d]$  code is called an optimum code.

If  $C$  is any  $[(q^k - 1)/(q - 1), k, q^{k-1}]$  code, then  $C$  is a Griesmer code and hence no coordinate of it is identically zero. Moreover if any two coordinates of  $C$  are equivalent then on applying row and column operations, if necessary any generator matrix for  $C$  can be put in the form

$$\left[ \begin{array}{cc|cccc} 1 & 1 & * & * & \dots & * \\ \hline 0 & 0 & & & & \\ \cdot & \cdot & & & & \\ \cdot & \cdot & & & & \\ 0 & 0 & & & & \end{array} \right] \quad , \text{ where } *'s \text{ are some elements in } GF(q).$$

Clearly  $G'$  generates  $[((q^k-1)/(q-1))-2, k-1, q^{k-1}]$  code.

But such a code does not exist as  $g_q(k-1, q^{k-1}) = ((q^k-1)/(q-1))-1$ .

So coordinates of  $C$  are inequivalent. This gives an independent proof of the following result of MacDonald (1960).

**Theorem 2.1.** Any  $[((q^k-1)/(q-1)), k, q^{k-1}]$  code is equivalent to  $S_k(q)$ .

## II. A. OPTIMUM CODES

$$\text{Let } s = \left\lfloor \frac{d}{2^{k-1}} \right\rfloor \text{ and let } s \cdot 2^{k-1} - d = \sum_{i=1}^p 2^{u_i-1},$$

where  $k > u_1 > u_2 > \dots > u_p > 0$ . Let  $G_k$  be a generator matrix for  $S_k$  and let  $U_i$  be a  $k \times (2^{u_i-1})$  submatrix of  $G_k$  of rank  $u_i$ ,  $1 \leq i \leq p$ . If

$$(2.3) \quad \sum_{i=1}^p u_i \leq sk,$$

then Solomon and Stiffler [41] have shown that the matrix

$$(2.4) \quad [(G_k | G_k | \dots | G_k) \setminus (U_1 | U_2 | \dots | U_p)] \\ \leftarrow s\text{-copies} \rightarrow$$

generates a binary  $[g(k,d), k, d]$  code. Further if

$$(2.5) \quad u_{i+1} = u_i - 1 \text{ for } i = s, s+1, \dots, p-1, u_p \in \{1, 2\}$$

and  $G$  is the matrix defined by

$$(2.6) \quad G = [(G_k | G_k | \dots | G_k) \setminus (U_1 | U_2 | \dots | U_t | U \quad T | R)], \\ \leftarrow s\text{-copies} \rightarrow$$

where (i)  $U$  is a  $k \times (2^u-1)$  submatrix of  $G_k$  of rank  $u$  ;

(ii)  $T$  is a  $k \times (u+1)$  submatrix of  $U$  of rank  $u$ , whose columns add upto the zero vector ;

- (iii)  $R$  as a set contains a nonzero vector, if  $d$  is odd and null set otherwise;
- (iv) no column occurs more than  $s$ -times among the deleted columns ;

then  $G$  generates a binary  $[g(k,d), k, d]$  code [3]. The most general result of this type is that of Belov [3].

**Proposition 2.2** [3]. For given  $k$  and  $d$  let  $s$  and  $u_i$ 's be as defined above. If  $\sum_{i=1}^{\min\{p, s+1\}} u_i \leq sk$  or  $u_{i+1} = u_i - 1$  for  $i = s, s+1, \dots, p-1$  and  $u_p \in \{1, 2\}$  then  $n(k, d) = g(k, d)$ .

Belov [3] conjectured that for  $s = 1$  conditions (2.3) and (2.5) are also necessary for the existence of a binary  $[g(k, d), k, d]$  code. His conjecture was proved in parts by Logacev [36], van Tilborg [42] and Helleseht [23] by showing that the only  $[g(k, d), k, d]$ ;  $d \leq 2^{k-1}$  codes that exist come from the constructions given by (2.4) or (2.6). In particular the result of Helleseht gives

**Proposition 2.3** [16]. For  $2^{k-1} - 2^{k-i} + 3 \leq d \leq 2^{k-1} - 2^{k-i-1} - 2^i$ ,  $1 \leq i \leq \lfloor (k-2)/2 \rfloor$ , the inequality ' $n(k, d) > g(k, d)$ ' holds and for the other values of  $d \leq 2^{k-1}$ ,  $n(k, d) = g(k, d)$ .

As a consequence of Proposition 2.2 Tilborg [42] derived that for a fixed  $k$  if

$$(2.7) \quad d > \lceil (-3 + \sqrt{8k+1})/2 \rceil 2^{k-1},$$

then  $n(k, d) = g(k, d)$ .

Further for  $s > 1$  Helleseth and van Tilborg [26] have constructed a new class of codes meeting the Griesmer bound for  $2^{k-1} + 2^{k-3} - 15 \leq d \leq 2^{k-1} + 2^{k-3} - 8$ ,  $k \geq 7$ . Thus above stated conjecture of Belov does not hold for  $s > 1$ . In [24] Helleseth gave a new description of binary Griesmer codes that includes the earlier constructions given by Solomon and Stiffler [41], Belov, Logachev and Sandimirov [4] and Helleseth and van Tilborg [26]. He also gave several new families of binary Griesmer codes that are not attainable by any of the previously known constructions.

If  $C$  is a  $[g_q(k,d)+t, k, d]$ ,  $t = 0$  or  $1$ ; code then Dodunekov has shown that there exists a generator matrix for  $C$  in which each row has weight  $d$  or  $d+t$  [12]. However for binary codes Dodunekov and Manev have proved the following general result

**Proposition 2.4** [16]. If  $C$  is a binary  $[n,k,d]$  code with  $n = g(k,d)+t$ , for some nonnegative integer  $t$ , then  $C$  has a generator matrix with each row having weight between  $d$  and  $d+t$ .

The case  $t = 0$  of Proposition 2.4 was first proved by Tilborg [42]. An easy consequence of Proposition 2.4 is the following

**Proposition 2.5** [16]. If  $C$  is a binary  $[g(k,d)+1, k, d]$  code with  $d = 2^m t$ ,  $3 \leq t < 2^{k-m-2} - 1$ , then  $\text{wt}(c) \equiv 0 \pmod{2^m}$  for every  $c \in C$ .

Following proposition summarizes the properties of a binary Griesmer code deduced by Busschbach, Gerretzen and van Tilborg [7], Dodunekov and Manev [15] and van Tilborg [12].

**Proposition 2.6.** Let  $C$  be  $[g(k,d), k, d]$  code. Then any generator matrix for  $C$  has no column repeated more than  $\lceil d/2^{k-1} \rceil$  times and some column repeated exactly  $\lceil d/2^{k-1} \rceil$  times. Moreover if  $d = 2^m \cdot t$ , then  $\text{wt}(c) \equiv 0 \pmod{2^m}$  for all  $c \in C$ .

Determining  $n_q(k,d)$  for given  $k$  and  $d$  in general is a difficult task. In recent years Baumert and McEliece [2], van Tilborg [43], Dodunekov and Manev [16] and many others have worked on determining  $n(k,d)$  for small values of  $k$ . If  $k \leq 4$  and  $d$  any positive integer then by Proposition 2.2  $n(k,d) = g(k,d)$ . However this is not the case for  $k \geq 5$ . Baumert and McEliece [2] have determined the value of  $n(k,d)$  for  $k = 5$  and  $6$ . In fact they proved the following

**Proposition 2.7 [2].**  $n(k,d) = g(k,d) + 1$  for  $k = 5, 3 \leq d \leq 6$  or  $k = 6, 3 \leq d \leq 14$  or  $19 \leq d \leq 20$ . For all other values of  $d$  with  $k = 5$  or  $6$ ,  $n(k,d) = g(k,d)$ .

van Tilborg [43] calculated  $n(7,d)$  for all values of  $d$  and gave several values of  $d$  for which  $n(7,d) = g(7,d) + 2$ . Some classes of binary codes satisfying the inequality ' $n(k,d) \geq g(k,d) + 2$ ' were determined by Dodunekov and

Manev [16]. Their results are summarized by following two propositions.

Proposition 2.8 [16]. If  $d \leq 2^k$  and  $n(k,d) \geq g(k,d)+t$ , then  $n(k+1,d) \geq g(k+1,d)+t$ .

Proposition 2.9 [16].  $n(k,d) \geq g(k,d) + 2$  for the following values of  $k$  and  $d$

- (i)  $d = 2^{k-i}, 2^{k-i}-2 ; 3 \leq i \leq k-4 ;$
- (ii)  $d = 3 \cdot 2^{k-i}, 3 \cdot 2^{k-i} - 2 ; 4 \leq i \leq k-4 ;$
- (iii)  $d = 5 \cdot 2^{k-i} (k \geq 9), 5 \cdot 2^{k-i}-2 (k \geq 10); 5 \leq i \leq k-2 ;$
- (iv)  $d = 7 \cdot 2^{k-i} (k \geq 7), 7 \cdot 2^{k-i}-2 (k \geq 8); 5 \leq i \leq k-1.$

They also determined bounds on  $n(8,d)$ , which were further improved by Dodunekov, Helleseeth, Manev and Ytrehus [14],[17]. In [27] Helleseeth and Ytrehus showed the nonexistence of some binary 8-dimensional codes by first proving the following two propositions.

Proposition 2.10 [27]. Let  $C$  be a binary  $[n,k,d]$  code and let  $\{B_i\}$ ,  $0 \leq i \leq n$ ; be the weight distribution of  $C^\perp$ . If  $B_i \neq 0$  then an  $[n-i, k-i+1, d]$  code exists.

Proposition 2.11 [27]. Let  $C$  be a binary code and let  $c_1, c_2 \in C$ . If  $c_1 = (1,1,\dots,1,0,0,\dots,0)$  and  $c_2 = (c_2^1 | c_2^0)$ ,  $c_2^0$  being part of  $c_2$  below the zero entries of  $c_1$ , then  $wt(c_1+c_2) = wt(c_1) - wt(c_2) + 2wt(c_2^0)$ .

The updated detailed information of bounds on  $n(8,d)$

can be obtained from the table of Verhoeff [44] on  $d_2[n,k]$ ,  $1 \leq k \leq n \leq 127$ .

Note that for  $k \leq 8$  there is no  $d > 2^{k-1}$  for which  $n(k,d) > g(k,d)$ . However this is not true for  $k \geq 9$  as Logachev [37] has proved that a binary  $[g(9,336), 9, 336]$  code does not exist.

Dodunekov [12] generalized (2.3) and (2.5) to codes over  $GF(q)$  and gave a set of sufficient conditions on  $k$ ,  $d$  and  $q$  for which  $n_q(k,d) = g_q(k,d)$ . The following three propositions summarize his results.

**Proposition 2.12 [12].** Let  $s = \lceil d/(q-1)q^{k-1} \rceil$  and let  $s(q-1)q^{k-1} - d = \sum_{i=0}^p a_i q^{u_i-1}$ ,  $k = u_0 > u_1 > \dots > u_p > 0$ ,  $0 \leq a_0 \leq q-2$ ,  $1 \leq a_i \leq q-1$  for  $1 \leq i \leq p$ . The optimum code meets the Griesmer bound if any one of the following holds.

$$(2.8) \quad a_0 = 0 \quad \text{and} \quad \sum_{i=1}^p u_i \leq sk ;$$

$$(2.9) \quad a_0 = 0, \quad u_{i+1} = u_i - 1, \quad \text{for } i = s, s+1, \dots, p-1, \quad \text{and} \\ n_q(u_s+1, d_1) = g_q(u_s+1, d_1) \quad \text{for} \\ d_1 = q^{u_p-1} + \sum_{i=s}^p (q-1-a_i) q^{u_i-1} ;$$

$$(2.10) \quad a_0 > 0 \quad \text{and} \quad s(q-1) \geq \sum_{i=0}^p a_i ;$$

$$(2.11) \quad d > [(k-2)(q-1) - (q-2)] q^{k-1} - 2q, \quad k \geq 3 ;$$

(2.12)  $q = 2^m$ ,  $k = 3$  and  $d \leq q+2$  ;

(2.13)  $q$  odd,  $k = 3$  and  $d \leq q+1$ , except for  $d=q$ .

**Proposition 2.13 [12].** If  $k \geq q \geq 3$  and  $2q^i < d \leq q^{i+1}$  for  $0 \leq i \leq k-q$ , then  $n_q(k,d) > g_q(k,d)$ .

**Proposition 2.14 [12].** If  $q|d$  and  $n_q(k,d) = g_q(k,d)$  then  $n_q(k,d-a) = g_q(k,d-a)$ , for all  $1 \leq a \leq q-1$ . Conversely if  $n_q(k,d-a) > g_q(k,d-a)$ , for some  $1 \leq a \leq q-1$  then  $n_q(k,d-b) > g_q(k,d-b)$ , for all  $0 \leq b \leq a$ .

## II.B. RESIDUAL CODE

For showing nonexistence of certain codes Tilborg introduced binary residual codes [43]. Dodunekov further extended it for codes over  $GF(q)$  [12]. Let  $C$  be an  $[n,k,d]$  code with generator matrix  $G$  and let  $c$  be the first row of  $G$ . Then the residual code of  $C$  with respect to  $c$  (denoted by  $\text{res}(C,c)$ ) is the code generated by the restriction of  $G$  to those columns where  $c$  has a zero entry. If only weight  $w$  of  $c$  is relevant we usually write  $\text{res}(C,w)$  for  $\text{res}(C,c)$ . For  $w < d + \lfloor w/q \rfloor$ ,  $\text{res}(C,w)$  is an  $[n-w, k-1, d_0]$ ,  $d_0 \geq d-w + \lfloor w/q \rfloor$  code [12].

The concept of a residual code is useful in many respects. For example :

1. To show the nonexistence of certain codes : Nonexistence of a binary  $[n,k,d]$  code with even  $d$  implies nonexistence



of any binary  $[n+2d, k+1, 2d]$  or  $[n+2d-3, k+1, 2d-2]$  code.

2. To find an upper bound for the minimum distance of certain binary cyclic codes : We need the following proposition.

**Proposition 2.15** [38 ; p.203]. If  $C$  is a binary  $[n, k, d]$  cyclic code with  $\delta-1$  consecutive zeros then  $d \geq \delta$ .

**Example 2.1** Let  $C$  be the  $[9, 7, d]$  binary cyclic code generated by  $g(x) = x^2 + x + 1$ . Then  $\delta = 2$  and so  $2 \leq d \leq 3$ .  $\text{Res}(C, 3)$  is a  $[6, 6, d_0]$  code. By the Griesmer bound  $1 \geq d_0 \geq d - \lfloor 3/2 \rfloor$ ; hence  $d = 2$ .

**Example 2.2** Let  $C$  be the  $[15, 9, d]$  binary cyclic code generated by  $g(x) = x^6 + x^4 + x^3 + x^2 + 1$ . Then  $\delta = 3$  and so  $3 \leq d \leq 5$ .  $\text{Res}(C, 5)$  is a  $[10, 8, d_0]$  code, where  $2 \geq d_0 \geq d - \lfloor 5/2 \rfloor$ ,  $d \leq 4$  (the actual value).

**Example 2.3** Let  $C$  be the  $[21, 12, d]$  binary cyclic code generated by  $g(x) = x^9 + x^8 + x^5 + x^4 + x^2 + x + 1$ . Then  $\delta = 5$  and so  $5 \leq d \leq 7$ . Now  $\text{res}(C, 7)$  is a  $[14, 11, d_0]$  code with  $2 \geq d_0 \geq d - \lfloor 7/2 \rfloor$ ; hence  $d = 5$ .

3. For showing uniqueness of certain binary codes with given weight distribution.

First part of the following theorem has been proved by J.E. MacDonald (IBM J. Res. Dev., 1960). However a simple proof is given for completeness.

**Theorem 2.2** Let  $C$  be a binary  $[n = n(k,d), k, d]$  code.

(i) If all nonzero vectors in  $C$  have weight  $d$  then for some positive integer  $t$ ,  $C$  is isomorphic to  $t \cdot S_k$  ( $t$ -copies of the Simplex code  $S_k$ ). (ii) If  $C$  has all one vector (denoted by  $\underline{1}$ ) and every other nonzero vector has weight  $d$  then  $C$  is isomorphic to  $t$ -copies of the first order Reed-Muller code of dimension  $k$  (denoted by  $t \cdot \text{RM}(1, k-1)$ ).

**Proof.** (i)  $d$  is even. For if  $d = 2m+1$ , then  $\text{res}(C, d)$  is an  $[n-d, k-1, d_0]$ ,  $d_0 \geq m+1$  code. Let  $c_1, c_2 \in C$ . Without loss of generality we can assume that  $c_1 = (1 \ 1 \ \dots 1 \ \overset{\leftarrow n-d \rightarrow}{0 \ 0 \ \dots 0})$  and let  $c_2 = (c_2^1 | c_2^0)$ , where  $c_2^1$  is the first part of  $c_2$  of length  $d$  and  $c_2^0$  is the remaining part of length  $n-d$ . Since  $c_2^0 \in \text{res}(C, d)$ ,  $\text{wt}(c_2^0) \geq m+1$  and hence  $\text{wt}(c_2^1) \leq m$  (as  $\text{wt}(c_2) = d$ ). Therefore  $\text{wt}(c_1 + c_2) = d - \text{wt}(c_2^1) + \text{wt}(c_2^0) \geq 2m+2$ , a contradiction. Let  $d = 2m$ . Then  $\text{res}(C, d)$  is an  $[n-d, k-1, m]$  code with all nonzero vectors having weight  $m$  and hence  $m$  is even. Proceeding this way we have  $d = 2^{k-1}t$  for some positive integer  $t$ . From Proposition 2.2 it is easy to see that  $n(k, d) = g(k, d) = t(2^k - 1)$ . No coordinate of  $C$  could be zero and every coordinate repeats at most  $t$  times as  $\lceil d/2^{k-1} \rceil = t$ . Further no coordinate of  $C$  repeats fewer than  $t$  times for otherwise  $n$  will be less than  $t(2^k - 1)$ . Hence  $C$  is isomorphic to  $t \cdot S_k$ .

(ii) Let  $G$  be a generator matrix for  $C$  with first row of weight  $n$  and let  $G'$  be the matrix  $G$  with first row deleted.

The code  $C'$  generated by  $G'$  is a single weight code.

Permuting columns of  $G'$  it may be written in the form

$$[G_{k-1}|G_{k-1}|\dots|G_{k-1}|0],$$

where  $G_k$  denotes a generator matrix of  $S_k$ . Thus  $d = t2^{k-2}$ .

MacWilliams equation for  $B_1$  gives  $n+(n-t2^{k-1})(2^k-2)+(n-2n) = 0$  or  $n = t2^{k-1}$ . Hence by definition of a first order Reed-Muller code,  $C$  is isomorphic to  $t.RM(1,k-1)$ .

### II.C. THE COVERING RADIUS PROBLEM

Let  $C$  be an  $[n,k,d]$  code. Then spheres of radius  $\lfloor d-1/2 \rfloor$  around codewords are disjoint, but they need not cover the whole space  $GF(q)^n$ . The smallest integer  $\rho$ , such that spheres of radius  $\rho$  around codewords cover the whole space is called the covering radius of the code. We will denote the covering radius of a code  $C$  by  $R(C)$ . A code  $C$  is called perfect if  $R(C) = \lfloor (d-1)/2 \rfloor$  and quasiperfect if  $R(C) = \lfloor (d-1)/2 \rfloor + 1$ . Many equivalent statements for the covering radius are known [8]. For example the covering radius of a code is

- (i) the weight of a maximum weight coset leader ;
- (ii) the least integer  $\rho$  such that any  $(n-k)$ -tuple over  $GF(q)$  (called Syndrome) is a linear combination of some  $\rho$  or fewer columns of any parity check matrix of the code.

Determining covering radius of a given code in

general is a difficult task. In recent years much work has been done on finding bounds for the covering radius of a code. For a survey of results on covering radius reader is referred to [8], [32]. Some of the results that are needed for our reference, are listed below for completeness.

If  $C$  is an  $[n, k, d]$  code and  $\rho$  is the least positive integer for which

$$(2.14) \quad \sum_{i=0}^{\rho} \binom{n}{i} (q-1)^i \geq q^{n-k},$$

then  $R(C) \geq \rho$ .

**Proposition 2.16** [8]. Appending an overall parity check or the zero parity check to the generator matrix of a given code increases the covering radius by one ; while puncturing a code on  $p$  coordinates reduces the covering radius by atmost  $p$ .

Let  $C_1$  and  $C_2$  be codes with dimensions  $k_1$  and  $k_2$  ( $k_1 \geq k_2$ ) and generator matrices  $G_1$  and  $G_2$  respectively. A code  $C$  is said to be a catenation of  $C_1$  and  $C_2$  if  $C$  has a generator matrix  $[G_1 | G'_2]$ , where  $G'_2$  is  $G_2$  with  $k_1 - k_2$  rows of zeros attached. The following proposition gives a lower bound on  $R(C)$  in terms of  $R(C_1)$  and  $R(C_2)$ .

**Proposition 2.17** [8]. If  $C$  is a catenation of two codes  $C_1$  and  $C_2$  then  $R(C) \geq R(C_1) + R(C_2)$ .

If a binary  $[n,k]$  code  $C$  has a generator matrix in the form

$$G = \left[ \begin{array}{c|c} G_0 & A \\ \hline 0 & G_1 \end{array} \right]$$

and if the codes generated by  $G_0$  and  $G_1$  are  $C_0$  and  $C_1$  respectively then Mattson [39] has proved the following relation between their covering radii.

**Proposition 2.18 [39].** Let  $C$ ,  $C_0$  and  $C_1$  be as defined above then  $R(C) \leq R(C_0) + R(C_1)$ .

A lower bound for the covering radius of an  $[n,k]$  code is  $t_q[n,k]$ , the minimal covering radius of any  $[n,k]$  code. This was first defined by Cohen, Karpovsky, Mattson and Schatz [8] for  $q = 2$ . Obviously  $t_q[n,k] \geq \rho$ , where  $\rho$  is given by (2.14). In [21] Graham and Sloane have given a table of bounds on  $t_2[n,k]$  for  $1 \leq k \leq n \leq 64$ .

A code  $C_1$  is called a subcode (supercode) of  $C$  if  $C_1 \subseteq C$  ( $C_1 \supseteq C$ ). Moreover  $C_1$  is said to be a subcode of codimension  $r$  of  $C$ , if there exist  $r$  distinct elements  $a_1, a_2, \dots, a_r \in C$ , such that  $C = \bigcup_{i=1}^r (a_i + C_1)$ ,  $(a_i + C_1) \cap (a_j + C_1) = \emptyset$ ,  $i \neq j$ . An  $[n,k,d]$  code  $C$  is called maximal if there does not exist a proper supercode of  $C$  with same  $n$  and  $d$ . A code  $C$  is maximal if and only if  $R(C) \leq d-1$  [8]. Dodunekov [12] has shown that any  $[n_q(k,d), k, d]$  code  $C$  is maximal and hence

(2.15)  $R(C) \leq d-1$ .

Many upper bounds on the covering radius of a binary code  $C$  are known [8]. The best known upper bound on the covering radius of an  $[n, k, d]$  code  $C$  is given by Janwa [34].

**Proposition 2.19** [34]. Let  $C$  be an  $[n, k, d]$  code, then

$$R(C) \leq n - \sum_{i=1}^k [d/q^i] = n - g_q(k, d) + d - [d/q^k] \equiv H_q(n, k, d).$$

If  $n = g_q(k, d)$ , then the above proposition immediately gives

$$(2.16) \quad R(C) \leq d - \left\lceil \frac{d}{q^k} \right\rceil.$$

The above inequality for  $q = 2$  was first proved by Busschbach, Berretzen and van Tilborg [7]. In [34] Janwa has extended the truth of (2.16) to any optimum code. Thus

**Proposition 2.20** [34]. If  $C$  is an  $[n_q(k, d), k, d]$  code then

$$R(C) \leq d - [d/q^k].$$

## II.D. NORMALITY OF CODES

Graham and Sloane [21], while looking for binary  $[n, k]$  codes with smaller covering radius, defined the concept of normality. This was generalized to nonbinary linear codes by Janwa [32].

Let  $C$  be an  $[n, k]$  code with none of the coordinate identically zero. Fix  $i \in \{1, 2, \dots, n\}$ . For  $\alpha \in GF(q)$ , let

$$C_{\alpha}^{(i)} = \{x \in C: \text{ith coordinate of } x \text{ is } \alpha\} \text{ and let}$$

$$N^{(i)} = \max_{\alpha \in GF(q)} \left\{ \sum_{x \in C_{\alpha}^{(i)}} d(x, C_{\alpha}^{(i)}) : x \in GF(q)^n \right\}.$$

Then  $N^{(i)}$  is called the norm of  $C$  with respect to the coordinate position  $i$ . Let  $N = \min_{1 \leq i \leq n} N^{(i)}$ .  $N$  is called the norm of  $C$ . The code is called normal if  $N \leq qR(C) + (q-1)$ .

With the above definition of the norm Theorems 6, 11 and 12 of Graham and Sloane [21] are false (M.C. Bhandari and M.S. Garg, IEEE Trans. Inform Theory, pp. 953-954, 1990).

However with a modified definition of norm given by Cohen, Robstein and Sloane [9] these results are true. In the modified definition  $N^{(i)}$  is defined as above and  $N$  is said to be a norm of the code if  $N \geq N^{(i)}$  for at least one coordinate  $i$ . This definition is puzzling as the authors of [9] at one place say "We deliberately do not insist that equality holds" and on the other place they say "Of course we always choose  $N$  as small as possible". Therefore the previous definition of the norm is better as one obtains the unique value of the norm for a given code.

The hypothesis of Lemma 27 in [21] proved by Graham and Sloane needs to be modified (M.C. Bhandari and M.S. Garg, IEEE Trans. Inform. Theory, pp. 653-654, 1990). Let  $F_i$  denotes the set of all binary  $n$ -tuples except  $\underline{0}$  and  $\underline{1}$  (the all zero and all one vector respectively) and let  $A_i \subseteq F_i$ ,  $A_i^c = F_i \setminus A_i$  ( $i = 1, 2$ ). Then the above lemma is stated as follows.

Proposition 2.21 [21]. If  $A_1$  and  $A_2$  satisfy

$$(A_i + A_i) \cup (A_i^c + A_i^c) \supset A_i^c \quad (i = 1, 2),$$

$$A_i + A_i^c \supset A_i \quad (i = 1, 2),$$

$$\underline{1} + A_1 = A_1,$$

$$\underline{1} \in A_2 + A_2^c$$

then the code with parity check matrix

$$\left[ \begin{array}{c|c|c|c} A_1 & A_1^c & 0 & 1 \\ \hline 0 & 1 & A_2 & A_2^c \end{array} \right]$$

has covering radius 2.

If we take  $m_1 = 3$ ,  $m_2 = 4$ ;  $A_1 = \{010, 001, 101, 110\}$  and  $A_2 = \{1101, 1110, 1100, 0111, 0101, 0110, 0100\}$ , then  $A_1$  and  $A_2$  satisfy all

the conditions of Proposition 2.20 but the vector  $(0001111)^{tr}$  can not be written as a sum of two columns of the parity check matrix given in Proposition 2.20.

However Proposition 2.20 is true if  $A_1$  and  $A_2$  in addition satisfy  $A_1 \in A_2 + A_2$ .

In a recent paper Hou (IEEE Trans. Inform. Theory, pp. 683-685, 1990) has proved the following upper bounds on the norm  $N$  of a code  $C$

$$(i) \quad N \leq 2R(C) + [d/2] - 1, (d \geq 3) \quad (ii) \quad N \leq 3R(C) - 2(R \geq 3).$$

The following theorem summarizes known sufficient conditions for a code to be normal [9],[31],[33].

**Proposition 2.22.** Let  $C$  be an  $[n, k, d]$  code and let  $H(C) = n_q(k, d) + d - [d/q^k]$ .  $C$  is normal if any one of the following holds

- i)  $q = 2$  and  $R(C_0^{(i)}) \leq R(C) + 2$ , for some  $i$ ;
- ii)  $q = 2$ ,  $R(C) = H(C)$  and  $d \leq 2^{k+1}$ ;
- iii)  $q = 2$ ,  $R(C) = H(C) - 1$  and  $d \leq 2^k$ ;
- iv)  $R(C_0^{(i)}) \leq R(C) + 1$ , for some  $i$ ;
- v)  $R(C) = H(C)$  and  $d \leq q^k$ .

In [35] Kilbay and Sloane proved that any binary  $[n, k, d]$  code is normal if either  $n \leq 14$  or  $k \leq 5$  or  $d \leq 5$ . However the case  $d=5$  is not true (X.Hou, IEEE Trans. Inform. Theory, pp. 683-685, 1990). They also gave examples of abnormal binary nonlinear codes. At present it is not known if an abnormal binary linear code exists.

## 1. E THE NUMBER $\max_s(r, q)$

A subset  $S$  of  $GF(q)^r$  having  $n$  elements is called an  $(n, s)$ -set if any  $s$  elements of  $S$  are linearly independent.



The largest value of  $n$  for which an  $(n,s)$ -set in  $GF(q)^r$  exists is denoted by  $\max_s(r,q)$  and a  $(\max_s(r,q),s)$ -set  $T$  is called complete. Determination of  $\max_s(r,q)$  is called the packing problem, first considered by Bose [6] for statistical interest and later (Bose 1961) for its connection with coding theory.

Determination of  $\max_s(r,q)$  in general is a difficult problem. It is known only in some special cases. A lower bound on  $\max_s(r,q)$  can be obtained by considering codes. If  $C$  is an  $[n,n-r,d]$  code then any  $d-1$  columns of a parity check matrix for  $C$  are linearly independent and so  $\max_{d-1}(r,q) \geq n$ . For  $n > r$  the converse is also true.

For  $s \geq 1$ ,  $\max_s(r,q)$  is a strictly increasing function of  $r$ . To see this let  $\max_s(r,q) = n$ . Writing vectors of an  $(n,s)$ -set in  $GF(q)^r$  as columns one gets an  $rxn$  matrix  $H = [x_1, x_2, \dots, x_n]$  in which any  $s$  columns are linearly independent. Moreover any  $s$  columns of the matrix

$$H' = \begin{bmatrix} x_1 & x_2 & \dots & x_n & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix}$$

are also linearly independent. Hence  $\max_s(r+1,q) > n$ .

The following two propositions summarize some known results on  $\max_s(r,q)$ .

Proposition 2.23 [28;Ch.14]. (i)  $\max_2(r,q) = (q^r-1)/(q-1)$ ,

$$(ii) \quad \max_3(3,q) = \begin{cases} q+1 & \text{if } q \text{ is odd} \\ q+2 & \text{if } q \text{ is even} \end{cases}$$

$$(iii) \quad \max_3(4,q) = q^2+1$$

(iv) If  $\max_{d-1}(r-1,q) < n \leq \max_{d-1}(r,q)$  then

$k_q[n,d] = n-r$ , where  $k_q[n,d] = \max \{k: \text{there exists an } [n,k,d] \text{ code} \}$ .

Proposition 2.24 [20]. For given  $r,q$  and  $d$ , suppose  $\max_d(r+1,q) \leq n$ ,  $\max_d(r,q) \leq m$  and  $\max_d(r^1+1,q) \leq n$  where  $r^1 = n-r-2$ ,  $d^1 = n-m-1$ . If  $n > n^1$  then  $\max_d(r+1,q) \leq n-1$ .

Games [20] has found bounds on  $\max_s(r,3)$  for  $r \leq 15$ , which were further improved by Hill [29]. For a survey of known results till 1983, concerning  $\max_s(r,q)$  we refer to Hirschfeld [30].

## CHAPTER III

### COVERING RADIUS OF OPTIMUM CODES

#### III.A. A LOWER BOUND

Let  $C$  be a  $[g(k,d), k, d]$  binary code with  $d \leq 2^{k-1}$ . Then columns of any generator matrix  $G$  for  $C$  are nonzero and distinct (Proposition 2.6). Hence  $C$  is a punctured binary Simplex code and so

$$\begin{aligned} R(C) &\geq R(S_k) - \text{number of columns deleted (Proposition 2.16)} \\ &= 2^{k-1} - 1 - (2^k - 1 - g(k,d)) = g(k,d) - 2^{k-1}. \end{aligned}$$

Thus one has

**Theorem 3.1.** If  $C$  is a binary  $[g(k,d), k, d]$  code with  $d \leq 2^{k-1}$  then  $R(C) \geq g(k,d) - 2^{k-1}$ .

The best lower bound on the covering radius of a binary  $[n,k]$  code is  $t[n,k]$ , the minimum covering radius of any binary  $[n,k]$  code [8]. A table of lower and upper bounds for  $t[n,k]$ ,  $1 \leq k \leq n \leq 64$  has been given by Graham and Sloane [21].

There are Griesmer codes for which the lower bound given by Theorem 3.1 is better than  $t[n,k]$ , restricted to Griesmer codes. For example if  $C$  is a  $[62,6,31]$  once punctured, once shortened first order Reed-Muller code then

$g(k,d)-2^{k-1} = 30$ , while  $23 \leq t[62,6] \leq 27$ . Table 3.1 below gives a list of Griesmer codes for which  $g(k,d)-2^{k-1} \geq t[n,k]$ . The existence of codes given in Table 3.1 follows from [2].

Table 3.1

| k | d  | $n = g(k,d)$ | $t[n,k]$ | $g(k,d)-2^{k-1}$ |
|---|----|--------------|----------|------------------|
| 3 | 4  | 7            | 2        | 3                |
| 4 | 6  | 12           | 4        | 4                |
| 4 | 8  | 15           | 5        | 7                |
| 5 | 14 | 28           | 11       | 12               |
| 5 | 16 | 31           | 13       | 15               |
| 6 | 26 | 53           | 19-22    | 21               |
| 6 | 28 | 56           | 20-24    | 24               |
| 6 | 30 | 60           | 22-26    | 28               |
| 6 | 32 | 63           | 23-27    | 31               |

### III.B. AN UPPER BOUND

Let  $C$  be an  $[n,k,d]$  code,  $n < n_q(k+1,d)$  and let  $x \in GF(q)^n$  with  $d(x,C) = R(C)$ . If  $R(C) \geq d+n+1-n_q(k+1,d)$  and if  $G$  is a generator matrix for  $C$ , then the matrix

$$\left[ \begin{array}{c|c} \overleftarrow{n_q(k+1,d)-n-1} \rightarrow & x \\ \hline 1 & 1 \cdot \cdot \cdot \cdot \cdot \cdot 1 \\ \hline 0 & G \end{array} \right]$$

generates an  $[n_q(k+1,d)-1, k+1, d]$  code. This contradicts the minimality of  $n_q(k+1,d)$  and the following theorem is proved.

**Theorem 3.2.** The covering radius  $R(C)$  of any  $[n,k,d]$  code  $C$  with  $n < n_q(k+1,d)$  satisfies  $R(C) \leq d+n-n_q(k+1,d)$ .

For any  $k$  and  $d$ ,  $n_q(k+1,d) > n_q(k,d)$  ; for if  $n_q(k+1,d) \leq n_q(k,d)$ , then an  $[n_q(k+1,d)-1, k, d]$  code can be obtained from an  $[n_q(k+1,d), k+1, d]$  code by deleting a suitable column from its parity check matrix, a contradiction. The number ' $n_q(k+1,d)-n_q(k,d)$ ' is a useful parameter in determining an upper bound for the covering radius of an optimum code, and will be denoted by  $b_q(k,d)$ , i.e.,

$$(3.1) \quad b_q(k,d) = n_q(k+1,d) - n_q(k,d).$$

For simplicity one often writes  $b(k,d)$  for  $b_2(k,d)$ . As shown above  $b_q(k,d) \geq 1$ . The following theorem shows that the multiplicity of a column in any generator matrix of an  $[n_q(k,d), k,d]$  code cannot exceed  $b_q(k-1,d)$ .

**Theorem 3.3.** Let  $G$  be a generator matrix of an  $[n_q(k,d), k,d]$  code. Then any column of  $G$  repeats atmost  $b_q(k-1,d)$  times.

**Proof.** If some column of  $G$  repeats  $b'$  times,  $b' > b_q(k-1,d)$ , then using row and column operations,  $G$  can be put in the form

$$\left[ \begin{array}{c|cccc} \overleftarrow{b'} & & & & \\ 1 & 1 & \dots & 1 & * & * & \dots & * \\ \hline & & & 0 & & & G' & \end{array} \right], \text{ where } *'s \text{ are some elements in } GF(q).$$

Clearly  $G'$  generates an  $[n, k-1, d]$  code ;  $n < n_q(k-1, d)$ , a contradiction to the minimality of  $n_q(k-1, d)$ .

**Corollary 3.1.** If  $b_q(k-1, d) = 1$ , then any generator matrix of an  $[n_q(k, d), k, d]$  code is a submatrix of the generator matrix of  $S_k(q)$ .

If  $C$  is an optimum code, then Theorem 3.2 gives the following upper bound for its covering radius.

**Corollary 3.2.** The covering radius of an  $[n_q(k, d), k, d]$  code  $C$  satisfies  $R(C) \leq d - b_q(k, d)$ .

A necessary and sufficient condition for equality in Corollary 3.2 is given by the following theorem.

**Theorem 3.4.** An  $[n_q(k, d), k, d]$  code has covering radius  $d - b_q(k, d)$  if and only if there exists an  $[n_q(k+1, d), k+1, d]$  code with  $b_q(k, d)$  equivalent coordinates.

**Proof.** Let  $C$  be an  $[n = n_q(k, d), k, d]$  code with covering radius  $d - b_q(k, d)$  and generator matrix  $G$ . Let  $x \in GF(q)^n$  such that  $d(x, C) = d - b_q(k, d)$ . Then the matrix

$$G' = \left[ \begin{array}{c|cccc} \overleftarrow{b_q(k, d)} & & & & \\ 1 & 1 & \dots & 1 & x \\ \hline & & & 0 & G \end{array} \right]$$

generates an  $[n_q(k+1,d), k+1, d]$  code with  $b_q(k,d)$  equivalent coordinates. Conversely if there exists an  $[n_q(k+1,d), k+1, d]$  code  $C'$  with  $b_q(k,d)$  equivalent coordinates then by row and column operations a generator matrix  $G'$  for  $C'$  can be put in the above form. Clearly  $G$  will generate an  $[n_q(k,d), k, d]$  code with  $d(x,C) \geq d - b_q(k,d)$ . Since  $C$  is optimum,  $R = d - b_q(k,d)$ .

### III.B.1. APPLICATIONS

1. The bound given by Corollary 3.2 is attained in many cases:

(i) Let  $C$  be any binary  $[21,5,10]$  code. Then  $b(5,10) = 2[2]$ . Since  $t[21,5] = 8[21]$ ,  $R(C) = 8$ .

(ii) Let  $C$  be any binary  $[16,5,8]$  code and let  $C'$  be the  $[15,5,7]$  once punctured code  $C$ . Since  $t[15,5] = 5[21]$  and  $b(5,7) = 2[2]$ ,  $R(C') = 5$ . Hence by Proposition 2.16,  $R(C) = 6$ .

2. The upper bound given by Corollary 3.2 is helpful in determining the covering radius of MacDonald codes.

**Theorem 3.5.** (i)  $R(C_{k;1}) = 2^{k-1} - 2$  ;  
(ii)  $R(C_{k;2}) = 2^{k-1} - 4$ ,  $k \geq 4$  ;  
(iii)  $2^{k-1} - 8 \leq R(C_{k;3}) \leq 2^{k-1} - 7$ ,  $k \geq 6$ .

**Proof.** By Theorem 3.1,  $R(C_{k;u}) \geq 2^k - 2^u - 2^{k-1} = 2^{k-1} - 2^u$ .

Since  $b(k, 2^{k-1}-1) = 1$  [16],  $b(k, 2^{k-1}-2) \geq 2$  for  $k \geq 4$  [16] and  $b(k, 2^{k-1}-4) \geq 3$  for  $k \geq 6$  [17; Lemma 4.2]. The

result follows from Corollary 3.2.

Corollary 3.3.  $b(k, 2^{k-1}-2) = 2$  and  $b(k, 2^{k-1}-4) \leq 4$ .

By techniques similar to those used in Theorem 3.5 lower and upper bounds on  $R(C_{k;u})$ , for any  $u$ ,  $1 \leq u \leq k-1$  can be found, but they are far away from each other for  $u \geq 4$ . It will be interesting to determine  $R(C_{k;u}(q))$ , in general.

3. A sufficient condition for the normality of optimum codes can be determined using Theorem 3.2.

Let  $C$  be an  $[n = n_q(k, d), k, d]$  code. Choose a codeword  $(c_1, c_2, \dots, c_n)$  of weight  $d$  and a coordinate  $i$  with  $c_i = 0$ . Recall that  $C_0^{(i)}$  denotes the set of all codewords with  $i$ th coordinate zero. Let  $D$  be the code obtained from  $C_0^{(i)}$  by deleting the  $i$ th coordinate.  $D$  is an  $[n-1, k-1, d]$  code. Moreover a parity check matrix  $H'$  for  $D$  can be obtained by deleting the  $i$ th column from a parity check matrix  $H$  of  $C$ . Since at least  $d-1$  columns of  $H'$  are required to write the deleted column;  $R(D) \geq d-1$ . So by Theorem 3.2  $R(D) = d-1$  and hence  $R(C_0^{(i)}) = d$  (Proposition 2.16). This proves the following lemma.

Lemma 3.1. Let  $C$  be an optimum code with minimum distance  $d$ , then there exists a coordinate  $i$  such that  $R(C_0^{(i)}) = d$ .



If  $k(C) = d-1$  or  $d-2$ , then the following two results follow from the above lemma and Proposition 2.22 ((i),(iv)).

Theorem 3.6. Optimum codes with covering radius  $d-1$  are normal.

Theorem 3.7. Binary optimum codes with covering radius  $d-1$  or  $d-2$  are normal.

It may be observed that if  $n(k,d) = g(k,d) + t$ ,  $t \in \{0,1\}$ ,  $d \leq 2^{k+1}$  ( $q > 2$ ,  $n_q(k,d) = g_q(k,d) + t$ ,  $\lceil d/q^k \rceil = t+1$ ) then Theorem 3.7 (Theorem 3.6) is a corollary to Proposition 2.22 (ii) and (iii) (Proposition 2.22 (v)).

### III.B.2. AN UPPER BOUND ON $b(k,d)$

In [1] Adams has shown that if  $C_0$  is any subcode of index two of a binary code  $C$ , then  $R(C) \geq \lceil R(C_0)/2 \rceil$ . Moreover if  $C$  is an optimum code with minimum distance  $d$  then by Lemma 3.1, there is a coordinate  $i$  such that  $R(C_0^{(i)}) = d$  and  $C_0^{(i)}$  is a subcode of index two. Thus

$$\lceil \frac{d}{2} \rceil \leq R(C) \leq d - b(k,d)$$

and the following theorem is proved.

Theorem 3.8.  $b(k,d) \leq \lceil d/2 \rceil$ .

So  $n(k+1,d)$  cannot be arbitrarily away from  $n(k,d)$ .

The above theorem can be improved further in some cases.

Theorem 3.9. If  $k \geq 2$  and  $d \geq 5$ , then  $b(k,d) \leq \lceil d/2 \rceil - 1$ .

Proof. Let  $C$  be a binary  $[n,k,d]$  optimum code. If  $d$  is odd and  $b(k,d) = \lceil d/2 \rceil$ , then by Corollary 3.2,  $R(C) = \lceil (d-1)/2 \rceil$

and hence  $C$  is perfect. So  $C$  must be any one of the following three types

- (i)  $[2^m-1, 2^m-m-1, 3]$  : Single error-correcting Hamming code;
- (ii)  $[23, 12, 7]$ : Golay code ;
- (iii)  $[n, 1, n]$  : Repetition code.

But  $C$  cannot be of type (i) or (iii) as  $k \geq 2$  and  $d \geq 5$ . So  $C$  must be a  $[23, 12, 7]$  Golay code. But  $b(12, 7) = 3$  [44], a contradiction. Since  $b(k, d-1) = b(k, d)$  for any even  $d$ , the assertion follows.

A sufficient condition for a binary optimum code to be quasiperfect is given by the following theorem.

**Theorem 3.10.** For given  $k$  and  $d$  if (i)  $k \neq 1, 12$  (ii)  $d=5$  or  $d \geq 9$ ,  $d$  odd and (iii)  $b(k, d) = \lfloor d/2 \rfloor - 1$ , then any binary  $[n(k, d), k, d]$  code  $C$  has covering radius  $d-b(k, d)$  and is quasiperfect.

**Proof.** If  $R(C) < d-b(k, d)$ , then the code is perfect, a contradiction. Therefore  $R(C) = d-b(k, d) = \lfloor (d-1)/2 \rfloor + 1$  and code is quasiperfect.

Since  $b(4, 5) = b(9, 5) = b(14, 5) = 2$  [44] , one has

**Corollary 3.4.** Binary  $[11, 4, 5]$ ,  $[17, 9, 5]$  and  $[23, 14, 5]$  codes are quasiperfect.

### III.B.3. PERFORMANCE

The bound given by Corollary 3.2 is better than the best known upper bound (Proposition 2.20).

**Theorem 3.11.** If  $n_q(k,d) = g_q(k,d)$  or  $d \leq q^k$  then  $d - b_q(k,d) \leq d - \lceil d/q^k \rceil$ . However if  $n_q(k,d) = g_q(k,d) + t$  and  $n_q(k+1,d) = g_q(k+1,d) + t_1$ ,  $0 \leq t < t_1$ ; then  $d - b_q(k,d) < d - \lceil d/q^k \rceil$ .

The bound given by Corollary 3.2 is best possible for  $b_q(k,d) = 1$ .

**Theorem 3.12.** If  $b_q(k,d) = 1$ , then there exists an  $[n = n_q(k,d), k, d]$  code with covering radius  $d-1$ .

**Proof.** Let  $r = n - k$ . Then  $\max_{d-1}(r, q) \geq n$ . If  $\max_{d-1}(r, q) = n$ , then  $\max_{d-1}(r, q) < n+1 \leq \max_{d-1}(r+1, q)$ . So by Proposition 2.23  $k_q(n+1, d) = k$ . Since  $b_q(k, d) = 1$ ,  $n_q(k+1, d) = n+1$  and so there exists an  $[n+1, k+1, d]$  code over  $GF(q)$ . Thus  $k_q[n+1, d] \geq k+1$ , a contradiction. Therefore  $\max_{d-1}(r, q) > n$ . Let  $S$  be a set of  $\max_{d-1}(r, q)$   $r$ -tuples over  $GF(q)$ , such that any  $d-1$  of them are linearly independent and let  $H$  be an  $rxn$  matrix whose columns are any  $n$  elements in  $S$ . Then the code  $C$  having  $H$  as a parity check matrix is an  $[n, k, d]$  code over  $GF(q)$ . As  $S$  contains more than  $n$  elements, there exists an  $r$ -tuple  $x$  in  $S$  which is not a linear combination of any  $d-2$  or fewer columns of  $H$ . So the covering radius  $R$  of  $C$  must be greater

than or equal to  $d-1$ . Since  $C$  is optimum ;  $R = d-1$ .

By Theorems 2.1 and 3.12 one gets an alternative proof for the following corollary.

Corollary 3.5.  $R(S_k) = 2^{k-1} - 1$ .

The bound given by Corollary 3.2 is not attained for  $b(k,d) = 3$ .

Example 3.1. Let  $C$  be the  $[32,6,16]$  first order Reed-Muller code. Then  $b(6,16) = 3$  as  $n(7,16) = 35$  [43]. The covering radius for  $C$  is 12 [5] and  $12 < d-b(k,d)$ .

It will be interesting to determine whether the bound given by Corollary 3.2 is reached for  $b(k,d) = 2$  or not.

### III.C. THE NUMBER $\max_s(r,q)$ AND ITS RELATION WITH OTHER PARAMETERS

An  $(n,s)$ -set  $S$  of  $GF(q)^T$  can be completed if there exists an  $(\max_s(r,q),s)$ -set  $T$  with  $S \subseteq T$ . The following theorem shows that there are  $(n,s)$ -sets of  $GF(q)^T$  which cannot be completed.

**Theorem 3.13.** Let  $C$  be an  $[n,k,d]$  code over  $GF(q)$  with  $n < \max_{d-1}(n-k,q)$  and  $R(C) \leq d-2$ . Then the set  $S$  of columns of any parity check matrix for  $C$  cannot be completed.

**Proof.** If  $x \in GF(q)^{n-k} \setminus S$ , then  $x$  can be written as a linear combination of some  $d-2$  or fewer elements of  $S$ . So

$S \cup \{x\}$  is not an  $(n+1, d-1)$ -set and hence  $S$  cannot be completed.

A binary  $[15, 5, 7]$  code  $C$  with  $R(C) = 5[18]$  satisfies the hypothesis of Theorem 3.13.

A complete set need not be unique.

Example 3.2. Let  $C$  be a  $[21, 5, 10]$  code. Since  $\max_q(16, 2) = 21$ , the set  $S$  consisting of columns of any parity check matrix of  $C$  is complete. As there are exactly two inequivalent  $[21, 5, 10]$  codes [42],  $S$  is not unique.

If for given  $k, d$  and  $q$ ,  $b_q(k, d)$  is large enough, the following theorem is useful in determining the value of  $\max_{d-1}(r, q)$  for certain values of  $r$ .

Theorem 3.14. For given  $k, d$  and  $q$ , let  $n_q(k, d) = n$  and let  $r = n - k$ . If  $b_q(k, d) \geq 2$  then  $\max_{d-1}(r+t, q) = n+t$  for  $0 \leq t \leq b_q(k, d)-2$  and  $\max_{d-1}(r+b_q(k, d)-1, q) > n+b_q(k, d)-1$ .

Proof. Let  $C$  be an  $[n, k, d]$  code with  $b_q(k, d) \geq 2$ . By appending zero columns to a generator matrix for  $C$  one gets  $[n+1, k, d], \dots, [n+b_q(k, d)-2, k, d]$  codes. However  $[n+1, k+1, d], \dots, [n+b_q(k, d)-1, k+1, d]$  codes do not exist. So  $\max_{d-1}(r+t, q) = n+t$  for  $0 \leq t \leq b_q(k, d)-2$ . Since an  $[n+b_q(k, d), k+1, d]$  code exists,  $\max_{d-1}(r+b_q(k, d)-1, q) > n+b_q(k, d)$ .

Relations among various parameters are explored in next two theorems.

Theorem 3.15. Let  $n = n_q(k, d)$  and let  $n - k = r$ . Then the following are equivalent

- (i)  $\max_{d-1}(r, q) = n$  ;
- (ii)  $k_q[n, d] = k_q[n+1, d] = k$  ;
- (iii)  $b_q(k, d) \geq 2$  ;
- (iv) every  $[n, k, d]$  code has covering radius  $\leq d-2$ .

Proof. (i)  $\Rightarrow$  (ii) Since  $\max_s(r, q)$  is an strictly increasing function of  $r$ ,  $\max_{d-1}(r-1, q) < n$  and  $\max_{d-1}(r+1, q) \geq n+1$ .

Applying Proposition 2.23 we get

$$k_q[n, d] = k_q[n+1, d] = k.$$

(ii)  $\Rightarrow$  (iii) If  $b_q(k, d) < 2$  then  $b_q(k, d) = 1$  and hence there exists an  $[n+1, k+1, d]$  code over  $GF(q)$  . So

$k_q[n+1, d] \geq k+1$ , a contradiction.

(iii)  $\Rightarrow$  (iv) Follows by Corollary 3.2.

(iv)  $\Rightarrow$  (i) Since  $n = n_q(k, d)$ ,  $\max_{d-1}(r, q) \geq n$  . If  $\max_{d-1}(r, q) > n$ , let  $S$  be a  $(\max_{d-1}(r, q), d-1)$ -set and let  $H$  be an  $r \times n$  matrix, whose columns are any  $n$  elements from  $S$ . The code  $C$  having  $H$  as a parity check matrix is an  $[n, k, d]$  code . Since  $n < \max_{d-1}(r, q)$ , there exists  $x \in S$  which is not a linear combination of any  $d-2$  or fewer columns of  $H$ . So  $R(C) \geq d-1$ , a contradiction.

Theorem 3.16. Let  $n, k$  and  $d$  be given and let  $n - k = r$ . Then the following are equivalent

- (i)  $n_q(k, d) = n$  ;
- (ii)  $d_q[n-1, k] < d_q[n, k] = d$  ;
- (iii)  $k_q[n-1, d] < k_q[n, d] = k$  ;
- (iv)  $\max_{d-1}(r-1, q)+1 < n \leq \max_{d-1}(r, q)$ .

Proof. (i)  $\Rightarrow$  (ii) Obviously  $d_q[n, k] \geq d$ . If  $d_q[n, k] = d' > d$ , then there exists an  $[n, k, d']$  code and hence  $n \geq n_q(k, d')$ . Note that  $n_q(k, d+1) > n_q(k, d)$ , for if  $n_q(k, d+1) \leq n_q(k, d)$ , then an  $[n_q(k, d+1)-1, k, d]$  code can be obtained from an  $[n_q(k, d+1), k, d+1]$  code by deleting a suitable column from its generator matrix, a contradiction to the minimality of  $n_q(k, d)$ . Hence

$$n \geq n_q(k, d') > n_q(k, d) = n,$$

a contradiction. Moreover  $d_q[n-1, k] < d$ , otherwise there exists an  $[n-1, k, d]$  code, a contradiction to the minimality of  $n_q(k, d)$ .

(ii)  $\Rightarrow$  (iii) Obviously  $k_q[n, d] \geq k$ . If  $k_q[n, d] > k$ , then an  $[n, k+1, d]$  code would exist which gives an  $[n-1, k, d]$  code, a contradiction as  $d_q[n-1, k] < d$ . Again the nonexistence of an  $[n-1, k, d]$  code implies  $k_q[n-1, d] < k$ .

(iii)  $\Rightarrow$  (iv) Since  $k_q[n-1, d] < k_q[n, d] = k$ , there exists an  $[n, k, d]$  code. But an  $[n-1, k, d]$  code does not exist. Therefore  $\max_{d-1}(r, q) \geq n$  and  $\max_{d-1}(r-1, q) < n-1$ .

(iv)  $\Rightarrow$  (i)  $n_q(k, d) \leq n$ , as there exists an  $[n, k, d]$  code. Since  $n-1 > \max_{d-1}(r-1, q)$ , an  $[n-1, k, d]$  code does not exist. Hence  $n_q(k, d) = n$ .

Corollary 3.6.  $n_q(k, 3) = k+r$ , where  $r$  satisfies

$$\frac{q^{r-1}-1}{q-1} - r + 1 < k \leq \frac{q^r-1}{q-1} - r, \quad r \geq 2.$$

Proof. By Proposition 2.23  $\max_2(r, q) = \frac{q^r-1}{q-1}$  and so  $\max_2(r-1, q) + 1 < k+r \leq \max_2(r, q)$ . The result follows by Theorem 3.16.

Theorem 3.17. Let  $C$  be an  $[n = n_q(k, 3), k, 3]$  code.

Then

$$R(C) = \begin{cases} 1 & \text{if } k = ((q^r-1)/(q-1)) - r \text{ for some } r \\ 2 & \text{otherwise.} \end{cases}$$

Proof. If  $k = ((q^r-1)/(q-1)) - r$  for some  $r$  then by Corollary 3.6  $n_q(k, 3) = ((q^r-1)/(q-1))$ . Let  $H$  be a parity check matrix for  $C$ . Then columns of  $H$  are nonzero and inequivalent. Hence  $C = H_r(q)$  and so  $R(C) = 1$ . On the other hand if

$$\frac{q^{r-1}-1}{q-1} - (r-1) < k < \frac{q^r-1}{q-1} - r \text{ then } n_q(k, 3) = \frac{q^r-1}{q-1} - t, \quad t \neq 0.$$

Since  $\sum_{i=0}^1 \binom{n}{i} (q-1)^i < q^{n-k}$ , by (2.14)  $R(C) \geq 2$ . Since  $C$  is optimum,  $R(C) = 2$ .

In [29] Hill has shown that  $13 \leq \max_6(9, 3) \leq 20$  and  $14 \leq \max_7(10, 3) \leq 21$ . These bounds are further improved by the following theorem.



**Theorem 3.18.**  $14 \leq \max_6(9,3) \leq 19$  and  $15 \leq \max_7(10,3) \leq 20$ .

**Proof.** Since  $\max_8(11,3) = 16$  [29], there exists a  $[16,5,9]$  code  $C$  over  $GF(3)$ . By deleting columns from a generator matrix of  $C$  one gets  $[15,5,8]$  and  $[14,5,7]$  codes over  $GF(3)$ . Hence  $15 \leq \max_7(10,3)$  and  $14 \leq \max_6(9,3)$ . As  $\max_6(8,3) = 11$  and  $\max_8(11,3) = 16$  [29] hypothesis of Proposition 2.24 is satisfied and hence  $\max_6(9,3) \leq 19$ . Similarly  $\max_7(10,3) \leq 20$ .

### III.D. BOUNDS ON $R(S_k(q))$

If  $q > 2$ , then almost nothing is known about the covering radius of  $S_k(q)$ . In [32] Janwa has posed this as an open problem. Lower and upper bounds on  $R(S_k(q))$  are determined in the present section.

#### III.D.1. UPPER BOUNDS ON $R(S_k(q))$

Observe that  $S_k(q)$  is an optimum code. Hence by (2.15) the following upper bound for  $R(S_k(q))$  is obtained.

**Theorem 3.19.**  $R(S_k(q)) \leq q^{k-1} - 1$ .

The bound given by the above theorem is attained if  $q$  is even and  $k = 2$ .

**Theorem 3.20.** If  $q$  is even then  $R(S_2(q)) = q-1$ .

**Proof.** Let  $q = 2^m$ . By Proposition 2.12,  $b_q(2, q) = 1$ . Hence by Theorem 3.12 there exists a  $[q+1, 2, q]$  code with

covering radius  $q-1$ . Since every  $[(q^k-1)/(q-1), k, q^{k-1}]$  code is  $\mathcal{S}_k(q)$ , the assertion follows.

The bound given by Theorem 3.19 can be improved in some cases.

**Theorem 3.21.** If  $q$  is odd then  $R(S_2(q)) \leq q-2$ .

**Proof.** By Proposition 2.12  $n_q(3, q) = q+3$ . Thus  $b_q(2, q) = 2$  and the result follows using Corollary 3.2.

The bound given by Theorem 3.21 is attained.

**Example 3.3.**  $S_2(5)$  is a  $[6, 2, 5]$  code over  $GF(5)$  with generator matrix

$$\begin{bmatrix} 0 & 1 & 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

It is easy to verify that for  $a = (2, 3, 4, 4, 1, 1) \in GF(5)^6$ ,  $wt(a + S_2(5)) = 3$  and hence  $R(S_2(5)) = 3$ .

**Theorem 3.22.**  $R(S_k(3)) \leq 3^{k-1}-2$  for  $k \geq 2$ .

**Proof.** If  $k \geq 2$  then  $n_3(k+1, 3^{k-1}) \geq g_3(k+1, 3^{k-1})+1 \geq g_3(k, 3^{k-1})+2$  (Proposition 2.13). Thus  $b_3(k, 3^{k-1}) \geq 2$  and hence by Corollary 3.2  $R(S_k(3)) \leq 3^{k-1}-2$ .

The bound given by Theorem 3.22 is attained for  $k = 2$  [32] and 3.

Example 3.4.  $R(S_3(3)) = 7$ .

$S_3(3)$  is a  $[13,3,9]$  code over  $GF(3)$  with generator matrix

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 0 & 1 & 1 & 2 & 0 & 0 & 1 & 1 & 2 & 0 & 1 & 1 & 2 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

For  $a = (1,2,2,1,1,2,1,2,1,2,1,2,2) \in GF(3)^{13}$ ,  $wt(a+S_3(3)) = 7$ .

Theorem 3.23.  $R(S_k(4)) \leq 4^{k-1}-2$ ,  $k \geq 3$ .

Proof. If  $k \geq 3$  then  $n_4(k+1,4^{k-1}) \geq g_4(k+1,4^{k-1})+1 \geq g_4(k,4^{k-1})+2$  (Theorem 5.4). So  $b_4(k,2^{k-1}) \geq 2$  and hence  $R(S_k(4)) \leq 4^{k-1}-2$ .

### III.D.2. LOWER BOUND ON $R(S_k(q))$

Let  $t_k(q)$  denote the maximum number of  $(-1)$ 's in any vector of  $S_k(q)$  and let  $\underline{1}$  denote the all one vector of length  $n = (q^k-1)/(q-1)$ ; then  $wt(\underline{1} + S_k(q)) = n - t_k(q)$ .

This gives the following lower bound for  $R(S_k(q))$ .

Theorem 3.24.  $R(S_k(q)) \geq n - t_k(q)$ .

A relation between  $t_m(q)$  and  $t_k(q)$  for  $m > k$  is given by the following lemma.

Lemma 3.2.  $t_m(q) = q^{m-k} t_k(q)$ .

Proof. Let  $GF(q) = \{0,1,\alpha_1,\alpha_2,\dots,\alpha_{q-2}\}$  and let  $G_k(q)$  be a generator matrix of the Simplex code  $S_k(q)$ . Then

$$G_{k+1}(q) = \left[ \begin{array}{c|c|c|c|c} 0 & 0 & \dots & 0 & 1 \\ \hline & G_k(q) & & 0 & \\ \hline & & 1 & 1 & \dots & 1 \\ \hline & & & G_k(q) & & \dots \\ \hline & & & & \dots & \alpha_{q-2} \alpha_{q-2} \dots \alpha_{q-2} \\ \hline & & & & & G_k(q) \end{array} \right]$$

is a generator matrix for  $S_{k+1}(q)$  and  $t_{k+1}(q)$

$= \max q t_k(q), ((q^k - 1)/(q - 1)) + 1$ . If  $t_k(q) \leq ((q^{k-1} - 1)/(q - 1))$ , then  $R(S_k(q)) \geq n - t_k(q) \geq q^{k-1}$ , a contradiction. So  $q t_k(q) > (q^k - 1)/(q - 1)$  and hence  $t_{k+1}(q) = q t_k(q)$ . Repeating this  $(m - k)$  times one gets

$$t_m(q) = q^{m-k} t_k(q).$$

Two equivalent Simplex codes may have different values of  $t_k(q)$ . So one needs to determine the minimal value of  $t_k(q)$  for given  $k$  and  $q$  to get a good lower bound on the covering radius.

Suppose for given  $q$  there exists a positive integer  $k_0$  and a vector  $a = (a_1, a_2, \dots, a_n)$  of weight  $n$  with

$$wt(a + S_{k_0}(q)) = R(S_{k_0}(q)).$$

Then multiplying the  $i$ th coordinate of  $S_{k_0}(q)$  by  $a_i^{-1}$  for  $1 \leq i \leq n$  one gets an equivalent code  $S'_{k_0}(q)$  for which  $t'_{k_0}(q)$ , the maximum number of  $(-1)$ 's in any codeword of  $S'_{k_0}(q)$ , satisfies

$$n - t'_{k_0}(q) = wt(\underline{1} + S'_{k_0}(q)) = wt(a + S_{k_0}(q)) = R(S_{k_0}(q)).$$

Hence by Lemma 3.2 one has

Theorem 3.25. Let  $k_0$  be as defined above. Then

$$R(S_k(q)) \geq n - q^{k-k_0} t_{k_0}'(q), \text{ for } k \geq k_0$$

III.D.3. BOUNDS ON  $R(S_k(q))$  for  $q = 3, 4$  and  $5$

If  $q = 3$ , then by Example 3.4,  $t_3'(3) = n - R(S_3(3)) = 6$  and hence using Theorem 3.25 one gets the following lower bound for  $R(S_k(3))$ .

Theorem 3.26.  $R(S_k(3)) \geq (2 \cdot 3^{k-1} - 3^{k-2} - 1)/2$ , for  $k \geq 3$ .

If  $q = 2^m$  and there exists a vector  $a$  of weight  $n$  satisfying  $\text{wt}(a + S_2(q)) = R(S_2(q))$ . Then by Theorems and 3.25 one gets

$$(3.2) \quad R(S_k(q)) \geq ((q-1)q^{k-1} - (q-2)q^{k-2} - 1)/(q-1), \text{ for } k \geq 2 \text{ and } q=2^m.$$

Theorem 3.27.  $R(S_k(4)) \geq (3 \cdot 4^{k-1} - 2 \cdot 4^{k-2} - 1)/3$ , for  $k \geq 2$ .

Proof. Let  $a = (\omega, \omega, \omega^2, \omega^2, \omega)$ , where  $GF(4) = \{0, 1, \omega, \omega^2\}$ .

It is easy to verify that  $\text{wt}(a + S_2(4)) = 3 = R(S_2(4))$ ,

where  $S_2(4)$  has generator matrix

$$\begin{bmatrix} 0 & 1 & 1 & \omega & \omega^2 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

The result follows from (3.2).

Theorem 3.28.  $R(S_k(5)) \geq (3 \cdot 5^{k-1} - 2 \cdot 5^{k-2} - 1)/4$ , for  $k \geq 2$ .

Proof. The assertion follows easily by Example 3.3 and Theorem 3.25.

## CHAPTER IV

### MINIMAL LENGTH OF 9-DIMENSIONAL BINARY LINEAR CODES

In [42] Tilborg has shown that if  $d > \lceil (-3 + \sqrt{8k+1})/2 \rceil 2^{k-1}$  then  $n(k,d) = g(k,d)$ . This bound is improved in Section A of the present chapter. Using the construction of binary Griesmer codes given by Helleseeth [21] and the above improvement the equality ' $n(k,d) = g(k,d)$ ' is shown to be true for  $d \geq 258$  except for  $324 \leq d \leq 336$ . Bounds on  $n(9,d)$  for  $d \leq 256$  are obtained first by using known results and then further improved by giving constructions or showing nonexistence of certain 9-dimensional binary linear codes. Note that if  $C$  is a binary  $[n,k,d]$  code with  $d$  odd then by adding an overall parity check one gets an  $[n+1, k, d+1]$  code. Thus  $n(k,d+1) \leq n(k,d)+1$ . But  $n(k,d+1) > n(k,d)$ , so  $n(k,d) = n(k,d+1)-1$ . Therefore one only needs to consider even values of  $d$ . Throughout this chapter an  $[n,k,d]$  code will mean a binary linear  $[n,k,d]$  code.

#### IV.A. $n(9,d)$ FOR $d > 256$

Tilborg [42] has shown that if  $d > \lceil (-3 + \sqrt{8k+1})/2 \rceil 2^{k-1}$  then  $n(k,d) = g(k,d)$ . In next two theorems this lower bound is improved. As defined earlier, let  $s = \lceil d/2^{k-1} \rceil$  and let  $s2^{k-1} = \sum_{i=1}^p 2^{u_i-1}$ ;  $k > u_1 > u_2 > \dots > u_p > 0$ .

Theorem 4.1.  $n(k,d) = g(k,d)$  for any  $d > (t-1)2^{k-1}$ ,  
 where  $t$  is the least positive integer satisfying  $(t+1)(t+2) \geq 2k$ ,  
 i.e.,  $t = \lceil (-3 + \sqrt{8k+1})/2 \rceil$ .

Proof. It suffices to show that the condition given by Below  
 (Proposition 2.2) is satisfied. Let  $s, u_i$ 's and  $p$  be as defined  
 above. Then  $s \geq t$  and

$$\sum_{i=1}^{t+1} u_i \leq \sum_{i=1}^{t+1} (k-i) = (t+1)k - \frac{(t+1)(t+2)}{2} \leq tk.$$

If  $p-1 < t$  then  $\sum_{i=1}^{\min\{p,s+1\}} u_i < pk \leq sk$ . If  $t \leq p-1 < s$  then

$$\sum_{i=1}^{\min\{p,s+1\}} u_i = \sum_{i=1}^{t+1} u_i + \sum_{i=t+2}^p u_i \leq tk + \sum_{i=t+2}^p (k-i) < (p-1)k < sk.$$

Also if  $p-1 \geq s$  then

$$\sum_{i=1}^{\min\{p,s+1\}} u_i = \sum_{i=1}^{t+1} u_i + \sum_{i=t+2}^{s+1} u_i \leq tk + \sum_{i=t+2}^{s+1} (k-i) < sk.$$

Let  $t$  be as defined in Theorem 4.1. If  $k \geq 9$  and  
 $t = s+1$ , let  $v_1, v_2, \dots, v_t$  be integers defined inductively as  
 follows.

$v_1$  is the largest integer  $u < k$  for which  $\sum_{i=1}^{\min\{u-2,s+1\}} (u-i) \leq sk$ .

Suppose  $v_1 > v_2 > \dots > v_{j-1}$  are defined for some  $j < t$ . Choose  
 $v_j$  to be the largest integer  $u < v_{j-1}$  for which

$$(4.1) \quad \sum_{i=1}^{\min\{u-2,s-j+2\}} (u-i) \leq sk - \sum_{i=1}^{j-1} v_i.$$

Finally let

$$(4.2) \quad v_t = sk - \sum_{i=1}^{t-1} v_i.$$

Observe that  $v_{t-1}$  is the largest integer satisfying

$$(i) \ v_{t-1} < v_{t-2} \text{ and } (ii) \ (v_{t-1}-3) \leq sk - \sum_{i=1}^{t-1} v_i. \text{ So}$$

$$0 < v_t < v_{t-1}.$$

Theorem 4.2.  $n(k,d) = g(k,d)$  for  $d \geq (t-1)2^{k-1} - v$ , where

$$v = 2^{v_1-1} + 2^{v_2-1} + \dots + 2^{v_t-1} + 2^{v_t-2} + \dots + 2; \ t, v_1, v_2, \dots, v_t \text{ are as defined above.}$$

Proof. If  $d > (t-1)2^{k-1}$ , then by Theorem 4.1  $n(k,d) = g(k,d)$ . For  $(t-1)2^{k-1} - v \leq d \leq (t-1)2^{k-1}$ ,  $s = t-1$  and so

$$\sum_{i=1}^p 2^{u_i-1} = s2^{k-1} - d = (t-1)2^{k-1} - d \leq v.$$

If  $\sum_{i=1}^p 2^{u_i-1} \geq \sum_{i=1}^t 2^{v_i-1}$ , then  $u_i = v_i$  for  $1 \leq i \leq t$  and hence

$$\sum_{i=1}^{\min\{p, s+1\}} u_i = \sum_{i=1}^t v_i = sk.$$

If  $\sum_{i=1}^p 2^{u_i-1} < \sum_{i=1}^t 2^{v_i-1}$ , then either (i) there exist

$$1 \leq b_1 < b_2 < \dots < b_p \leq t-1 \text{ with } \sum_{i=1}^p 2^{u_i-1} = \sum_{i=1}^p 2^{v_{b_i}-1} \text{ or}$$

(ii) there exist  $1 \leq b_1 < b_2 < \dots < b_j \leq t-1$  with



$\sum_{i=1}^{j-1} 2^{v_{b_i}-1} < \sum_{i=1}^p 2^{u_i-1} < \sum_{i=1}^j 2^{v_{b_i}-1}$ . In case (i) holds

$u_i = v_{b_i}$  for  $1 \leq i \leq p$  and hence  $\sum_{i=1}^{\min\{p, s+1\}} u_i = \sum_{i=1}^p v_{b_i} < sk$ .

In case (ii) holds  $u_i = v_{b_i}$  for  $1 \leq i \leq j-1$  and

$u_{j-1+k} \leq v_{b_j} - k$ , for  $k = 1, 2, \dots, v_{b_j} - 2$  and hence

$$\sum_{i=1}^{\min\{p, s+1\}} u_i \leq \sum_{i=1}^{j-1} v_{b_i} + \sum_{i=1}^{\min\{v_{b_j}-2, s-j+2\}} (v_{b_j} - i) \leq sk.$$

Thus in any case  $\sum_{i=1}^{\min\{p, s+1\}} u_i \leq sk$  and hence the result follows by Proposition 2.2.

In particular if  $k = 9$ , the above theorem gives

**Corollary 4.1.**  $n(9, d) = g(9, d)$  for  $d \geq 338$ .

**Proof.** For  $k = 9$ ;  $t = 3$ ,  $v_1 = 8$ ,  $v_2 = 6$ ,  $v_3 = 4$  and hence  $v = 174$  and  $(t-1)2^{k-1} - v = 338$ .

If  $d = 258$  or  $314 \leq d \leq 322$ , then by Proposition 2.2,  $n(9, d) = g(9, d)$ . On the other hand if  $306 \leq d \leq 314$  then Helleseeth and Tilborg [26] have shown that  $n(9, d) = g(9, d)$ . Hence the remaining cases for  $d \geq 258$  are  $260 \leq d \leq 304$  and  $324 \leq d \leq 336$ .

For constructing codes meeting the Griesmer bound for  $k = 9$ ,  $260 \leq d \leq 304$  we need the following construction of an anticode given by Helleseeth [24].

Let  $C$  be an  $[n, k]$  code with generator matrix  $G$  and let

$$G' = [s_k | s_k | \dots | s_k] \setminus G.$$

The code  $C'$  generated by  $G'$  is called an anticode of  $C$  [19].

On the other hand if  $G'$  is any matrix and if maximum multiplicity of any column of it is  $s$  then

$$G = [\underbrace{s_k | s_k | \dots | s_k}_{\leftarrow s\text{-copies} \rightarrow}] \setminus G'$$

generates a code  $C$  having  $C'$ , the code generated by  $G'$ , as an anticode. Whenever  $G$  (or  $C$ ) and  $G'$  (or  $C'$ ) are used they are related as above.

For any  $k > u_1 > u_2 > \dots > u_p > 0$ , let  $n' = \sum_{i=1}^p (2^{u_i} - 1)$  and let  $\mathcal{C}_f(u_1, u_2, \dots, u_p)$  be the set of all  $k \times n'$  matrices  $G'$  for which the distance between any two codewords of  $C'$  is at most  $\sum_{i=1}^p 2^{u_i} - 1$ . If  $G' \in \mathcal{C}_f(u_1, u_2, \dots, u_p)$  and the corresponding  $G$  has rank  $k$  then Helleseth has shown that the code generated by  $G$  is a Griesmer code. Infact he proved the following

**Proposition 4.1 [24].** If  $G' \in \mathcal{C}_f(u_1, u_2, \dots, u_p)$  and if  $G$  generates a code  $C$  of dimension  $k$  then  $C$  is a Griesmer code with parameters  $[s(2^k - 1) - \sum_{i=1}^p (2^{u_i} - 1), k, s \cdot 2^{k-1} - \sum_{i=1}^p 2^{u_i-1}]$ .

This can be used to construct a  $[g(9, 260), 9, 260]$  code. Note that  $g(9, 260) = 524$  and  $2(2^9 - 1) - g(9, 260) = 498 = \sum_{i=1}^6 (2^{u_i} - 1)$  with  $u_1 = 8, u_2 = 7, u_3 = 6, u_4 = 5, u_5 = 4, u_6 = 3$ . For each  $u, 1 \leq u \leq 9$ , let  $\hat{U}(9, u)$  be the set of all  $u$ -dimensional

subspace of  $GF(2)^9$  and let  $U(9,u) = \{\hat{U} \setminus \{0\} : U \in U(9,u)\}$ .

Let  $V_1^{(1)} \dots V_6^{(1)}$  be matrices defined by

$$V_1^{(1)} = \left[ \begin{array}{cccc|cccc} 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \hline & U_1 \setminus W_1 & & & & W_1 & & \end{array} \right], \quad \begin{array}{l} U_1 \in U(8,8), W_1 \in U(8,4), W_1 \subseteq U_1 \\ \text{and every element in } W_1 \text{ has} \\ \text{zeros at the last four positions,} \end{array}$$

$$V_2^{(1)} = \left[ \begin{array}{cccc|cccc} 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \hline & U_2 \setminus W_2 & & & & W_2 & & \end{array} \right], \quad \begin{array}{l} U_2 \in U(7,7), W_2 \in U(7,4), W_2 \subseteq U_2 \\ \text{and elements in } W_2 \text{ have zeros} \\ \text{at 2nd, 3rd and 4th positions,} \end{array}$$

$$V_3^{(1)} = \left[ \begin{array}{cccc|cccc} 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \hline & U_3 \setminus W_3 & & & & W_3 & & \end{array} \right], \quad \begin{array}{l} U_3 \in U(6,6), W_3 \in U(6,4), W_3 \subseteq U_3 \\ \text{and elements of } W_3 \text{ have} \\ \text{zeros at the last two} \\ \text{positions,} \end{array}$$

$$V_4^{(1)} \in U(9,4) \text{ such that } \hat{V}_4^{(1)} \text{ is generated by the vectors} \\ (000001001)^{tr}, (100000011)^{tr}, (000011111)^{tr}, \\ (000100010)^{tr} \text{ and } (000010001)^{tr},$$

$$V_5^{(1)} \in U(9,4) \text{ such that } \hat{V}_5^{(1)} \text{ is generated by the vectors} \\ (001000100)^{tr}, (000100010)^{tr}, \\ (000010001)^{tr} \text{ and } (010000000)^{tr}$$

$$\text{and } V_6^{(1)} \in U(9,3) \text{ such that } \hat{V}_6^{(1)} \text{ is generated by the three vectors} \\ (000001001)^{tr}, (000010010)^{tr} \text{ and} \\ (000100100)^{tr}.$$

CENTRAL LIBRARY  
UNIVERSITY OF KANSAS

Acc. No. A.1140.34

If  $\alpha = [v_1^{(1)} | v_2^{(1)} | v_3^{(1)} | v_4^{(1)} | v_5^{(1)} | v_6^{(1)}]$  then it is easy to check that  $\alpha_1 \in \mathcal{C}_f(8,7,6,5,4,3)$  and no column occurs more than twice. So  $G_1 = [S_9 | S_9] \setminus G_1'$  generates a  $[524, 9, 260]$  code (Proposition 4.1).

On replacing  $\hat{v}_5^{(1)}$  and  $\hat{v}_6^{(1)}$  by their respective subspaces one also obtains the following codes

| Parameters of $C_1$ | $G_1'$ belongs to            |
|---------------------|------------------------------|
| $[528, 9, 262]$     | $\mathcal{C}_f(8,7,6,5,4,2)$ |
| $[531, 9, 264]$     | $\mathcal{C}_f(8,7,6,5,4)$   |
| $[536, 9, 266]$     | $\mathcal{C}_f(8,7,6,5,3,2)$ |
| $[539, 9, 268]$     | $\mathcal{C}_f(8,7,6,5,3)$   |
| $[543, 9, 270]$     | $\mathcal{C}_f(8,7,6,5,2)$   |
| $[546, 9, 272]$     | $\mathcal{C}_f(8,7,6,5)$     |

Thus the following theorem is proved.

**Theorem 4.3.** If  $260 \leq d \leq 272$  then  $n(9, d) = g(9, d)$ .

Now consider the case  $273 \leq d \leq 288$ . Define  $v_1^{(2)}, v_2^{(2)}, \dots, v_6^{(2)}$  by

$$v_1^{(2)} = \left[ \begin{array}{ccc|ccc} 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \hline & & & U_1 \setminus W_1 & & & & W_1 \end{array} \right], \text{ and the vectors of } W_1 \text{ have zeros at the last three positions,}$$

$U_1 \in U(8, 8), W_1 \in U(8, 5), W_1 \subseteq U_1$

$$V_2^{(2)} = \left[ \begin{array}{ccc|ccc} 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \hline & & U_2 \setminus W_2 & & & W_2 & & \end{array} \right], \quad \begin{array}{l} U_2 \in U(7,7), W_2 \in U(7,5), \\ W_2 \subseteq U_2 \text{ and the vectors} \\ \text{of } W_2 \text{ have zeros at 2nd} \\ \text{and 3rd positions,} \end{array}$$

$$V_3^{(2)} = \left[ \begin{array}{ccc|ccc} 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \hline & & U_3 \setminus W_3 & & & W_3 & & \end{array} \right], \quad \begin{array}{l} U_3 \in U(6,6), W_3 \in U(6,5), \\ W_3 \subseteq U_3 \text{ and each element} \\ \text{of } W_3 \text{ has first entry} \\ \text{zero,} \end{array}$$

$V_4^{(2)} \in U(9,4)$  such that  $\hat{V}_4^{(2)}$  is generated by the vectors  
 $(1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)^{tr}$ ,  $(0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0)^{tr}$ ,

$(1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)^{tr}$  and  $(0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0)^{tr}$ ,

$V_5^{(2)} \in U(9,3)$  such that  $\hat{V}_5^{(2)}$  is generated by the vectors

$(0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1)^{tr}$ ,  $(0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0)^{tr}$  and

$(1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1)^{tr}$

and  $V_6^{(2)} \in U(9,2)$  such that  $\hat{V}_6^{(2)}$  is generated by the two vectors

$(0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0)^{tr}$  and  $(1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1)^{tr}$ .

If  $G_2' = [V_1^{(2)} \mid V_2^{(2)} \mid V_3^{(2)} \mid V_4^{(2)} \mid V_5^{(2)} \mid V_6^{(2)}]$  then

$G_2' \in \mathcal{C}(8,7,6,4,3,2)$  and no column occurs more than twice.

So the code generated by the matrix  $G_2 = [S_9 \mid S_9] \setminus G_2'$  is  
a  $[552, 9, 274]$  Griesmer code. Deleting appropriate columns

from  $V_4^{(2)}$ ,  $V_5^{(2)}$  and  $V_6^{(2)}$  one also gets Griesmer codes for

$276 \leq d \leq 288$ .

Similarly if  $V_1^{(3)}, \dots, V_6^{(3)}$  are defined by

$$V_1^{(3)} = \left[ \begin{array}{cccc|cccc} 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \hline & U_1 & & W_1 & & & & W_1 \end{array} \right], \quad \begin{array}{l} U_1 \in U(8,8), W_1 \in U(8,6), \\ W_1 \subseteq U_1, \text{ vectors of } W_1 \\ \text{have zeros at the last} \\ \text{two positions,} \end{array}$$

$$V_2^{(3)} = \left[ \begin{array}{cccc|cccc} 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \\ \hline & U_2 & & W_2 & & & & W_2 \end{array} \right], \quad \begin{array}{l} U_2 \in U(7,7), W_2 \in U(7,6), \\ W_2 \subseteq U_2, \text{ each element of} \\ W_2 \text{ has 4th entry zero,} \end{array}$$

$V_3^{(3)} \in U(9,5)$ , vectors of  $V_3^{(3)}$  have zeros at the 4th, 5th 6th and 7th positions,

$V_4^{(3)} \in U(9,4)$  such that  $\hat{V}_4^{(3)}$  is generated by the vectors  
 $(1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)^{tr}$ ,  $(1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0)^{tr}$ ,  
 $(0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0)^{tr}$  and  $(0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1)^{tr}$ ,

$V_5^{(3)} \in U(9,3)$  such that  $\hat{V}_5^{(3)}$  is generated by the vectors  
 $(1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0)^{tr}$ ,  $(0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1)^{tr}$  and  
 $(0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0)^{tr}$ ,

$V_6^{(3)} \in U(9,2)$  such that  $\hat{V}_6^{(3)}$  is generated by the vectors  
 $(1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0)^{tr}$  and  $(1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1)^{tr}$

and  $G_3' = [V_1^{(3)} | V_2^{(3)} | V_3^{(3)} | V_4^{(3)} | V_5^{(3)} | V_6^{(3)}]$  then  $G_3 = [S_9 | S_9] \setminus G_3'$  generates a  $[g(9,290), 9, 290]$  code. Deleting appropriate columns from  $V_4^{(3)}$ ,  $V_5^{(3)}$  and  $V_6^{(3)}$  one gets Griesmer codes for  $292 \leq d \leq 304$ .

Hence the following theorem is proved.

Theorem 4.4. If  $273 \leq d \leq 304$  then  $n(9,d) = g(9,d)$ .

#### IV.B. KNOWN BOUNDS ON $n(9,d)$ FOR $d \leq 256$

By Proposition 2.3,  $n(9,d) = g(9,d)$  for  $d \leq 256$  except for  $3 \leq d \leq 126$ ,  $131 \leq d \leq 188$  and  $195 \leq d \leq 216$ . For each of these cases  $n(9,d) \geq g(9,d)+1$ . Table 4.1 below gives known bounds on  $n(9,d)$ . The lower bound is obtained by showing nonexistence of certain codes, the Table I of Verhoeff [44] or Proposition 2.8. Upper bounds are obtained by (i) Table I of Verhoeff [44] for  $3 \leq d \leq 58$  ( $d[n,k] \geq d$  implies  $n(k,d) \leq n$ ) ; (ii) Theorem 3.1 of [16] for  $131 \leq d \leq 188$  and  $195 \leq d \leq 216$ . The values of  $n(8,d)$  are taken from [14],[16],[17] and [27].

Table 4.1

| d  | $g(9,d)$ | $n(9,d)$ | d  | $g(9,d)$ | $n(9,d)$ |
|----|----------|----------|----|----------|----------|
| 4  | 13       | 14       | 22 | 48       | 50-52    |
| 6  | 17       | 18       | 24 | 51       | 53-55    |
| 8  | 20       | 21       | 26 | 56       | 58-60    |
| 10 | 25       | 27       | 28 | 59       | 61-63    |
| 12 | 28       | 30       | 30 | 63       | 65-67    |
| 14 | 32       | 34-35    | 32 | 66       | 69-70    |
| 16 | 35       | 38-39    | 34 | 73       | 74-77    |
| 18 | 41       | 43-45    | 36 | 76       | 77-80    |
| 20 | 44       | 46-48    | 38 | 80       | 82-85    |

| d  | $g(9,d)$ | $n(9,d)$   | d   | $g(9,d)$ | $n(9,d)$   |
|----|----------|------------|-----|----------|------------|
| 40 | 83       | 85-87      | 80  | 162      | $\geq 164$ |
| 42 | 88       | 89-94      | 82  | 168      | $\geq 169$ |
| 44 | 91       | 93-96      | 84  | 171      | $\geq 172$ |
| 46 | 95       | 97-100     | 86  | 175      | $\geq 177$ |
| 48 | 98       | 100-102    | 88  | 178      | $\geq 180$ |
| 50 | 104      | 106-109    | 90  | 183      | $\geq 185$ |
| 52 | 107      | 109-113    | 92  | 186      | $\geq 188$ |
| 54 | 111      | 113-116    | 94  | 190      | $\geq 192$ |
| 56 | 114      | 116-118    | 96  | 193      | $\geq 195$ |
| 58 | 119      | 121-126    | 98  | 200      | $\geq 202$ |
| 60 | 122      | $\geq 124$ | 100 | 203      | $\geq 205$ |
| 62 | 126      | $\geq 129$ | 102 | 207      | $\geq 209$ |
| 64 | 129      | $\geq 132$ | 104 | 210      | $\geq 212$ |
| 66 | 137      | $\geq 138$ | 106 | 215      | $\geq 217$ |
| 68 | 140      | $\geq 141$ | 108 | 218      | $\geq 220$ |
| 70 | 144      | $\geq 145$ | 110 | 222      | $\geq 224$ |
| 72 | 147      | $\geq 148$ | 112 | 225      | $\geq 227$ |
| 74 | 152      | $\geq 153$ | 114 | 231      | $\geq 233$ |
| 76 | 155      | $\geq 156$ | 116 | 234      | $\geq 236$ |
| 78 | 159      | $\geq 161$ | 118 | 238      | $\geq 240$ |



| d   | $g(v, d)$ | $n(9, d)$  | d   | $g(9, d)$ | $n(9, d)$ |
|-----|-----------|------------|-----|-----------|-----------|
| 120 | 241       | $\geq 243$ | 168 | 328       | 339-341   |
| 122 | 246       | $\geq 248$ | 170 | 343       | 344-346   |
| 124 | 249       | $\geq 251$ | 172 | 346       | 347-349   |
| 126 | 253       | 254        | 174 | 350       | 351-352   |
| 132 | 268       | 269        | 176 | 353       | 354-355   |
| 134 | 272       | 273        | 178 | 359       | 360-362   |
| 136 | 275       | 276        | 180 | 362       | 363-365   |
| 138 | 280       | 281-282    | 182 | 366       | 367-368   |
| 140 | 283       | 284-285    | 184 | 369       | 370-371   |
| 142 | 287       | 288-290    | 186 | 374       | 375       |
| 144 | 290       | 291-292    | 188 | 377       | 378       |
| 146 | 296       | 297-298    | 196 | 395       | 396       |
| 148 | 299       | 300-301    | 198 | 399       | 400       |
| 150 | 303       | 304        | 200 | 402       | 403       |
| 152 | 306       | 307        | 202 | 407       | 408       |
| 154 | 311       | 312-314    | 204 | 410       | 411       |
| 156 | 314       | 315-318    | 206 | 414       | 415-416   |
| 158 | 318       | 319-321    | 208 | 417       | 418-419   |
| 160 | 321       | 322-324    | 210 | 423       | 424       |
| 162 | 328       | 329-331    | 212 | 426       | 427       |
| 164 | 331       | 332-334    | 214 | 430       | 431       |
| 166 | 335       | 336-337    | 216 | 433       | 434       |

IV.C. UPPER BOUNDS ON  $n(9,d)$  FOR CERTAIN VALUES OF  $d$ 

Let  $C$  be a binary  $[n, k, d]$  maximal code with  $R(C) \geq R_0$  and generator matrix  $G$ . Then the matrix

$$\begin{array}{c|cccc} & \xleftarrow{d-R_0} & & & \\ \hline x & 1 & 1 & \dots & 1 \\ \hline G & & & & 0 \end{array}$$

generates an  $[n+d-R_0, k+1, d]$  code where  $x \in GF(q)^n$  such that  $d(x, C) = R(C)$ . This proves the following theorem.

**Theorem 4.5.** If  $C$  is a binary  $[n, k, d]$  maximal code with  $R(C) \geq R_0$ , then there exists an  $[n+d-R_0, k+1, d]$  code.

If  $G$  is a generator matrix for an  $[n, k, d]$  code with first row having weight  $d$  then on deleting any  $i (< d)$  columns, which have a nonzero entry in the first row, one obtains an  $[n-i, k, d-i]$  code. This proves the following theorem.

**Theorem 4.6.** Any  $[n, k, d]$  code gives an  $[n-i, k, d-i]$  code for  $i < d$ .

Let  $C$  be the  $[128, 8, 64]$  Reed-Muller code. Then  $R(C) = 56$  [40]. Applying Theorems 4.5 and 4.6 to  $C$  one gets  $[136, 9, 64]$ ,  $[134, 9, 62]$  and  $[132, 9, 60]$  codes.

**Corollary 4.2.**  $n(9, 64) \leq 136$ ,  $n(9, 62) \leq 134$  and  $n(9, 60) \leq 132$ .

If  $C$  is an  $[n = 128 + n(7, d-64), 8, d]$  code with  $66 \leq d \leq 92$ , then Dodunekov and Manev [16] have shown that there exists a

generator matrix  $G$  for  $C$  of the form

$$G = \left[ \begin{array}{c|cccc} & 0 & 0 & \dots & 0 \\ G_1 & & & & \\ & & G_2 & & \end{array} \right]$$

where  $G_1$  generates the  $[128,8,64]$  first order Reed-Muller code  $C_1$  and  $G_2$  generates an  $[n(7,d-64), 7, d-64]$  code  $C_2$ . Further if  $n(7,d-64) = n(8,d-64)-1$ , then  $C_2$  can be chosen to have  $k(C_2) = d-65$  (Theorem 3.12). As  $C$  is a catenation of  $C_1$  and  $C_2$ , by Proposition 2.17,  $R(C) \geq R(C_1) + R(C_2) = 56+d-65 = d-9$ . Therefore by Theorem 4.5 there exists an  $[n+9,9,d]$  code. This proves the following Theorem.

**Theorem 4.7.** If  $n(8,d-64) = n(7,d-64)+1$ ,  $64 < d \leq 92$  then  $n(9,d) \leq n(7,d-64) + 137$ .

**Corollary 4.3.**  $n(9,66) \leq 145$ ,  $n(9,68) \leq 149$ ,  $n(9,70) \leq 153$ ,  $n(9,72) \leq 156$ ,  $n(9,80) \leq 172$ ,  $n(9,86) \leq 184$  and  $n(9,88) \leq 187$ .

**Proof.** From tables of Tilborg [43] and of Dodunekov and Manev [16] it is easy to see that  $n(8,d-64) = n(7,d-64)+1$  for  $d = 66, 68, 70, 72, 80, 86$  and  $88$ . Hence the assertion follows from Theorem 4.7.

**Theorem 4.8.**  $n(9,100) \leq 216$ .

**Proof.** Let  $C$  be a  $[203,8,100]$  code with generator matrix  $G$  of the form

$$G = \left[ \begin{array}{c|cc|cc} G_1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ & & & & & 0 & 0 & \dots & 0 \\ & & G_2 & & & & & & \\ & & & & & & G_3 & & \end{array} \right],$$

where  $G_1, G_2, G_3$  generate  $[128, 8, 64]$ ,  $[64, 7, 32]$  and  $[11, 6, 4]$  codes  $C_1, C_2$  and  $C_3$  respectively [16]. Since  $R(C_1) = 56[40]$ ,  $n(C_2) = 28[8]$  and  $C_3$  can be chosen to have  $R(C_3) = 3$ , by Proposition 2.17

$$R(C) \geq R(C_1) + R(C_2) + R(C_3) = 87.$$

A  $[216, 9, 109]$  code can be constructed from  $C$  using Theorem 4.5.

The following upper bounds on  $n(9, d)$  for remaining values of  $d$ ,  $60 \leq d \leq 124$  are obtained by applying Theorem 4.6 to  $[184, 9, 86]$ ,  $[172, 9, 80]$ ,  $[216, 9, 100]$  and  $[254, 9, 126]$  codes.

Table 4.2

| $d$ | Upper bound<br>on $n(9, d)$ | $d$ | Upper bound<br>on $n(9, d)$ | $d$ | Upper bound<br>on $n(9, d)$ |
|-----|-----------------------------|-----|-----------------------------|-----|-----------------------------|
| 74  | 166                         | 96  | 212                         | 112 | 240                         |
| 76  | 168                         | 98  | 214                         | 114 | 242                         |
| 78  | 170                         | 102 | 230                         | 116 | 244                         |
| 82  | 180                         | 104 | 232                         | 118 | 246                         |
| 84  | 182                         | 106 | 234                         | 120 | 248                         |
| 90  | 206                         | 108 | 236                         | 122 | 250                         |
| 92  | 208                         | 110 | 238                         | 124 | 252                         |
| 94  | 210                         |     |                             |     |                             |

#### IV.D. NONEXISTENCE OF CERTAIN CODES

An improvement of the Griesmer bound for small distances was given by Dodunekov and Manev (Proposition 2.9). In case  $k \geq 9$ , the following theorem gives a further improvement.

**Theorem 4.9.** If  $3 \leq i \leq k-4$ ,  $k \geq 9$ , then  $n(k, 2^{k-i}) \geq g(k, 2^{k-i}) + 3$ .

**Proof.** The assertion is proved by induction, first on  $k$  for  $i = 3$  and then on  $i$ . Let  $i = 3$ . If  $k = 9$  then by Table 4.1  $n(9, 64) \geq g(9, 64) + 3$ . Let  $k > 9$ . If  $C$  is a  $[g(k, 2^{k-3}) + 2, k, 2^{k-3}]$  code, then  $\text{res}(C, 2^{k-3})$  is a  $[g(k-1, 2^{k-4}) + 2, k-1, 2^{k-4}]$  code, a contradiction to the induction hypothesis. Suppose  $i > 3$  and that the statement is true for  $i-1$  and any  $k \geq 9$ . For any  $k > 9$ ,  $n(k-1, 2^{k-i}) = n(k-1, 2^{k-1-(i-1)}) \geq g(k-1, 2^{k-1-(i-1)}) + 3$ . Hence by Proposition 2.8  $n(k, 2^{k-i}) \geq g(k, 2^{k-i}) + 3$ . If  $k = 9$ , then  $i = 4$  or  $5$ . By Table 4.1  $n(9, 32) \geq g(9, 32) + 3$  and  $n(9, 16) \geq g(9, 16) + 3$ .

Another lower bound for  $n(k, d)$  for certain values of  $d$  is given by the following theorem.

**Theorem 4.10.** Let  $d = 2^{k-4} - 2^m$ ,  $k \geq 10$ ,  $m \geq 0$ . Then  $n(k, d) \geq g(k, d)$ .

For the proof of the above theorem one needs the following four lemmas.

**Lemma 4.1.**  $n(9, 24) \geq 54$ .



possible for any  $x$  as only possible nonzero weights in  $C$  are 24, 32, 50. Hence  $A_{50} = 0$ .

$B_2 \leq 1$ . For, if  $B_2 \geq 2$ , then any generator matrix for  $C$  can be put in one of the following forms

$$\left[ \begin{array}{ccc|ccc} * & * & \dots & * & 1 & 1 & 1 \\ \hline & & & & G_1 & & 0 \end{array} \right] \quad \text{or} \quad \left[ \begin{array}{ccc|ccc} * & * & \dots & * & 1 & 1 & 0 & 0 \\ * & * & \dots & * & 0 & 0 & 1 & 1 \\ \hline & & & & G_2 & & 0 \end{array} \right] \quad \text{where } *'s \text{ are some elements, in } GF(2).$$

But then  $G_1$  will generate a  $[50, 8, 24]$  code and  $G_2$  will generate a  $[49, 7, 24]$  code, a contradiction [44]. MacWilliams equations for  $B_0$ ,  $B_1$  and  $B_2$  are

$$(4.3) \quad A_{24} + A_{32} + A_{34} + A_{36} + A_{40} + A_{44} + A_{48} = 511$$

$$(4.4) \quad -5A_{24} + 11A_{32} + 15A_{34} + 19A_{36} + 27A_{40} + 35A_{44} + 43A_{48} = 53$$

$$(4.5) \quad -7A_{24} + 17A_{32} + 13A_{34} + 77A_{36} + 169A_{40} + 293A_{44} + 449A_{48} = 256B_2 - 689.$$

If  $A_{48} \neq 0$ , then  $A_{48} = 1$ ,  $A_{36} = A_{44} = 0$ . A linear combination of (4.3) and (4.4) gives  $4A_{32} + 5A_{34} = 640$ .

So  $A_{34} = 4k$  for some nonnegative integer  $k$ . Solving (4.3), (4.4) and (4.5) simultaneously one gets  $1408 + 8k = 256B_2$ , a contradiction as  $B_2 \leq 1$ . So  $A_{48} = 0$ .

If  $C$  has a codeword  $c_1$  of weight 44, then  $\text{res}(C, c_1)$  is a  $[9, 8, 2]$  code having a vector  $c_2^0$  of weight 4. Let  $c_2 = (c_2^1 | c_2^0) \in C$ . By Proposition 2.11

$$\text{wt}(c_1 + c_2) = \text{wt}(c_1) + 2\text{wt}(c_2^0) - \text{wt}(c_2) = 52 - \text{wt}(c_2),$$

which is not possible. Therefore  $A_{44} = 0$ .

Finally multiplying (4.3) by  $(-1/8)$ , (4.4) by  $(-3/8)$ , (4.5) by  $(1/4)$  and adding one gets

$$5A_{32} + 12A_{36} + 32A_{40} = -256 + 64B_2 \leq -192,$$

a contradiction. Hence  $n(9,24) \geq 54 = g(9,24)+3$ .

Corollary 4.4.  $n(10,48) \geq 102 = g(10,48) + 3$ .

Proof. If  $C$  is any  $[101,10,48]$  code, then  $\text{res}(C,48)$  is a  $[53,8,24]$  code.

Lemma 4.2. Let  $d = 2^m t$  ( $m \geq 2$ ),  $2 \nmid t$  and let  $C$  be an  $[n,k,d]$  code. If  $C$  has a generator matrix with all rows having weight  $d$  and if  $\text{res}(C,d)$  has all weights divisible by  $2^{m-1}$ , then  $\text{wt}(c) \equiv 0 \pmod{2^m}$  for all  $c \in C$ .

Proof. Let  $c_1, c_2 \in C$ ,  $\text{wt}(c_1) = \text{wt}(c_2) = d$ . W.l.o.g. one can assume that  $c_1$  and  $c_2$  have the following configuration

$$c_1 = (1 \ 1 \ \dots \ 1 \ 0 \ 0 \ \dots \ 0)$$

$$c_2 = (c_2^1 | c_2^0).$$

Since  $c_2^0 \in \text{res}(C,d)$ ,  $2^{m-1} | \text{wt}(c_2^0)$ . Therefore  $2^{m-1} | \text{wt}(c_1 * c_2)$  and hence  $\text{wt}(c_1 + c_2)$  is divisible by  $2^m$ .

Dodunekov [13] has proved the nonexistence of a  $[116,9,56]$  code. An independent proof using the above lemma is given below.



Lemma 4.3.  $n(9,56) \geq 117$ .

Proof. Suppose there exists a  $[116,9,56]$  code  $C$ . Since  $116 = g(9,56)+2$ , by Proposition 2.4  $C$  has a generator matrix with rows having weights 56,57 or 58.  $A_{57} = 0$ .

For, if  $A_{57} \neq 0$ , then  $\text{res}(C,57)$  is a  $[59,8,28]$  code which does not exist [16]. Similarly  $A_{58} = 0$ .  $\text{Res}(C,56)$  is a  $[60,8,28]$  code. Since  $60 = g(8,28) + 2$ ,  $\text{res}(C,56)$  has a generator matrix with rows having weights 28,29 or 30.

But it cannot have a vector of weight 29 as then

$\text{res}(\text{res}(C,56),29)$  is a  $[31,7,14]$  code, which does not exist [43]. Therefore all weights in  $\text{res}(C,56)$  are even and hence by Lemma 4.2 all weights in  $C$  are divisible by

4. Thus possible nonzero weights in  $C$  are 56,64,68,80,96,112 and 116.  $B_2 = 0$ . For, if  $B_2 \neq 0$ , then by Proposition 2.10

there exists a  $[114,8,56]$  code, a contradiction as

$n(8,56) = 115$  [14]. MacWilliams equations for  $B_0$ ,  $B_1$  and  $B_2$  are

$$(4.6) \quad A_{56} + A_{64} + A_{68} + A_{80} + A_{96} + A_{112} + A_{116} = 511$$

$$(4.7) \quad -A_{56} + 3A_{64} + 5A_{68} + 11A_{80} + 19A_{96} + 27A_{112} + 29A_{116} = 29$$

$$(4.8) \quad -25A_{56} + 7A_{64} + 71A_{68} + 455A_{80} + 1415A_{96} + 2887A_{112} + 3335A_{116} = -33$$

If  $A_{116} \neq 0$ , then  $A_{116} = 1$ ,  $A_{64} = A_{68} = A_{80} = A_{96} = A_{112} = 0$  and hence (4.7) gives  $A_{56} = 0$ , a contradiction. Similarly if  $A_{112} \neq 0$ , then  $A_{112} = 1$ ,  $A_{68} = A_{80} = A_{96} = 0$ . Solving (4.6)

and (4.7) simultaneously one gets  $A_{56} = 382$ ,  $A_{64} = 128$  ; but these values do not satisfy (4.8). Therefore

$$A_{116} = A_{112} = 0.$$

If  $C$  has a vector of weight 96, then it is easy to verify that the  $[20,8,8]$  code  $C^0 = \text{res}(C, 96)$  has unique weight distribution  $A_0^0 = 1$ ,  $A_8^0 = 130$ ,  $A_{12}^0 = 120$  and  $A_{16}^0 = 5$ . Let  $c_2 = (c_2 | c_2^0) \in C$  with  $c_2^0 \in C^0$ . Then  $\text{wt}(c_2^0) \in \{8, 12, 16\}$ . Since  $\text{wt}(c_1 + c_2) = \text{wt}(c_1) + 2\text{wt}(c_2^0) - \text{wt}(c_2)$ , possible choices for  $\text{wt}(c_2)$  for given value of  $\text{wt}(c_2^0)$  are

|                    |    |          |    |
|--------------------|----|----------|----|
| $\text{wt}(c_2^0)$ | 8  | 12       | 16 |
| $\text{wt}(c_2)$   | 56 | 56 or 64 | 64 |

Therefore  $A_{68} = A_{80} = 0$  and  $A_{96} = 1$ . Solving (4.6) and (4.7) one gets  $A_{56} = 380$ ,  $A_{64} = 130$ , which do not satisfy (4.8). Hence  $A_{96} = 0$ .

A linear combination of (4.6), (4.7) and (4.8) (with  $A_{116} = A_{112} = A_{96} = 0$ ) gives

$$48A_{68} + 384A_{80} = 5120.$$

This is impossible as  $3 \nmid 5120$ . Hence a  $[116, 9, 56]$  code does not exist.

Lemma 4.4.  $n(10, 60) \geq 126$ .

Proof. If  $n(9, 60) \geq 125$  then by Proposition 2.8,  $n(10, 60) \geq 12$ . So one only needs to consider the case  $n(9, 60) < 125$ . Let

$C$  be a  $[124, 9, 60]$  optimum code. Proceeding on the same lines as in the proof of Lemma 4.3 it is easy to verify that all weights in  $C$  are divisible by 4. Thus possible nonzero weights in  $C$  are 60, 64, 72, 76, 88, 104, 120 and 124.

$B_2 = 0$ . For if  $B_2 \neq 0$ , then by Proposition 2.10 there exists a  $[122, 8, 60]$  code. But  $n(8, 60) \geq 123$  [27]. MacWilliams equations for  $B_0$ ,  $B_1$  and  $B_2$  are

$$(4.9) \quad A_{60} + A_{64} + A_{72} + A_{76} + A_{88} + A_{104} + A_{120} + A_{124} = 511$$

$$(4.10) \quad A_{60} + A_{64} + 5A_{72} + 7A_{76} + 13A_{88} + 21A_{104} + 29A_{120} + 31A_{124} = 31$$

$$(4.11) \quad 27A_{60} + 27A_{64} - 69A_{72} - 165A_{76} - 645A_{88} - 1733A_{104} - 3333A_{120} - 3813A_{124} = 3813.$$

$A_{124} = 0$ . For, if  $A_{124} \neq 0$ , then  $A_{124} = 1$ ,  $A_{72} = A_{76} = A_{88} = A_{104} = A_{120} = 0$  and hence solving (4.9) and (4.10) one gets  $A_{60} - A_{64} = 255$ , but these values do not satisfy (4.11). With a similar reasoning  $A_{120} = 0$ .

If  $A_{104} \neq 0$ , then  $A_{104} = 1$ ,  $A_{88} = 0$  and hence solving (4.9) and (4.11) one gets

$$96A_{72} + 192A_{76} = 8224.$$

This is not possible as  $3 \nmid 8224$ . So  $A_{104} = 0$ .

If  $A_{88} = 0$  and  $A_{76} = 0$  then solving (4.9), (4.10) and (4.11) one gets  $A_{64} = -41$ , a contradiction. So either  $A_{88} \neq 0$ , or  $A_{88} = 0$ ,  $A_{76} \neq 0$ . If  $A_{88} \neq 0$  then  $C^\circ = \text{res}(C, 88)$

is a  $[36, 8, 16]$  code for which  $b(8, 16) \geq 2$  (Table 4.1). Hence by Corollary 3.2  $R(C^0) \leq 14$ . Permuting columns, if necessary, any generator matrix for  $C$  can be put in the form

$$\left[ \begin{array}{c|c} \begin{array}{c} \overleftarrow{88} \rightarrow \\ 1 \ 1 \dots 1 \end{array} & \begin{array}{c} 0 \ 0 \dots 0 \end{array} \\ \hline G' & G^0 \end{array} \right], \quad G^0 \text{ is a generator matrix for } C^0.$$

So by Proposition 2.18,  $K(C) \leq \lfloor \frac{88}{2} \rfloor + R(C^0) \leq 58$ .

On the other hand if  $A_{88} = 0$ ,  $A_{76} \neq 0$ , then  $\text{res}(C, 76)$  is a  $[48, 8, 22]$  code  $C^0$  for which  $b(8, 22) \geq 2$  (Table 4.1). Therefore by Corollary 3.2,  $R(C^0) \leq 20$ .

Following the same procedure as above one gets

$K(C) \leq \lfloor \frac{76}{2} \rfloor + R(C^0) \leq 58$ . Thus in any case by Theorem 3.12, a  $[125, 10, 60]$  code does not exist.

**Proof of the Theorem 4.10.** The assertion is proved using induction on  $m$ . If  $k = 10$ , then  $0 \leq m \leq 5$ . For  $m = 0, 1$  or  $5$ , Table 4.1 and Proposition 2.8 give  $n(10, 64-2^m) \geq g(10, 64-2^m)+3$ . If  $m = 2$  or  $4$ , then by Lemma 4.4 and Corollary 4.4  $n(10, 64-2^m) \geq g(10, 64-2^m) + 3$ . Finally for  $m = 3$ , Proposition 2.8 and Lemma 4.3 give  $n(10, 56) \geq g(10, 56)+3$ .

Take  $m > 0$ ,  $k > 10$  and suppose the statement is true for  $m-1$ . Let  $C$  be a  $[g(k, 2^{k-4}-2^m)+2, k, 2^{k-4}-2^m]$  code. Then  $\text{res}(C, d)$  is a  $[g(k-1, 2^{k-5}-2^{m-1})+2, k-1, 2^{k-5}-2^{m-1}]$  code, which does not exist by the assumption.



But then  $C^0$  has a codeword of weight 48, a contradiction as  $A_{48}^0 = 0$ . Thus  $C$  does not exist.

**Theorem 4.12.**  $n(9,112) \geq 228$ .

**Proof.** Suppose there exists a  $[227,9,112]$  code  $C$ . Proceeding on the same lines as in the proof of Lemma 4.3 it is easy to verify that all weights in  $C$  are divisible by 4. So possible nonzero weights in  $C$  are 112, 128, 176 and 224. MacWilliams equations for  $B_0, B_1$  and  $B_2$  are

$$(4.14) \quad A_{112} + A_{128} + A_{176} + A_{224} = 511$$

$$(4.15) \quad -3A_{112} + 29A_{128} + 125A_{176} + 221A_{224} = 227$$

$$(4.16) \quad -1.9A_{112} + 307A_{128} + 7699A_{176} + 24307A_{224} = -25651 + 512B_2.$$

If  $A_{224} \neq 0$ , then  $A_{224} = 1$ ,  $A_{120} = A_{176} = 0$  and hence (4.14) and (4.15) do not have a common solution, a contradiction. So  $A_{224} = 0$ .

If  $A_{176} \neq 0$ , then  $A_{176} = 1$ . Solving (4.14) and (4.15) simultaneously one gets  $A_{128} = 51$  and  $A_{112} = 459$ , but then (4.16) gives  $B_2 = -2$ , a contradiction. Hence  $A_{176} = 0$ .

Solving (4.14), (4.15) and (4.16) for  $B_2$ , one gets  $B_2 = -14$ , a contradiction. Therefore  $[227,9,112]$  code does not exist.

**Theorem 4.13.**  $n(9,176) = 355$ .

**Proof.** Suppose a  $[354,9,176]$  code  $C$  exists. Proceeding on

on the same lines as in the proof of Lemma 4.3 it is easy to verify that possible nonzero weights in  $C$  are 176, 192, 224, 228 and 352.

If  $C$  has a codeword  $c_1$  of weight 352 and if  $c_2$  is any codeword of weight 176 then permuting coordinates if necessary they must have the following configuration

$$\begin{array}{l} 1 \ 1 \dots\dots\dots 1 \ 0 \ 0 \ c_1 \\ 1 \ 1 \dots 1 \ 0 \ 0 \dots 0 \ 0 \ 0 \ c_2 \end{array}$$

For, if the last two coordinates of  $c_2$  are 10, 01 or 11 then  $\text{wt}(c_1 + c_2) = 178$  or 180, a contradiction. Since  $C$  has a generator matrix in which every row has weight 176, last two coordinates of  $C$  are identically zero and hence  $n(\cdot, 176) \leq 352$ , a contradiction to Table 4.1. Hence  $A_{352} = 0$ .

MacWilliams equations for  $B_0, B_1$  and  $B_2$  are

$$(4-17) \quad A_{176} + A_{192} + A_{224} + A_{228} = 511$$

$$(4-18) \quad -A_{176} + 15A_{192} + 47A_{224} + 51A_{228} = 177$$

$$(4-19) \quad 175A_{176} - 273A_{192} - 4241A_{224} - 5025A_{228} = 62481 - 512B_2$$

If  $A_{228} \neq 0$ , then  $A_{228} = 1$ . For, if  $A_{228} \geq 2$ , let  $c_1, c_2 \in C$  with  $\text{wt}(c_1) = \text{wt}(c_2) = 228$ . Permuting coordinates, if necessary it can be assumed that they have the following configuration

$$\begin{array}{l} 1 \ 1 \dots\dots\dots 1 \ 0 \ 0 \dots\dots\dots 0 \ c_1 \\ 1 \ 1 \dots 1 \ 0 \ 0 \dots 0 \ 1 \ 1 \dots 1 \ 0 \ 0 \dots 0 \ c_2 \\ \quad \quad \quad \leftarrow x \rightarrow \quad \leftarrow x \rightarrow \end{array}$$

Then  $\text{wt}(c_1 + c_2) = 2x$  and hence  $x \in \{88, 96, 112, 114\} = A$ . Moreover if  $c_2 = (c_2^1 | c_2^0)$ , then  $c_2^0$  is a vector in  $\text{res}(C, c_1)$  of weight  $x$ . So  $\text{res}(\text{res}(C, c_1), x)$  is a  $[126-x, 7, 62 - \lfloor \frac{x}{2} \rfloor]$  code which does not exist for any  $x \in A[43]$ . Similarly  $A_{224} = 0$ . A linear combination of (4.17) and (4.18) give  $16A_{192} = 636$ , a contradiction. Therefore  $A_{228} = 0$ .

$A_{224} = 0$ . For if,  $A_{224} \neq 0$ , then as above  $A_{224} = 1$ . Solving (4.17), (4.18) and (4.19) one gets  $B_2 = -9$ , a contradiction.

Thus  $A_i = 0$  for  $i \geq 224$  and the equations (4.17), (4.18) and (4.19) give  $B_2 = -15$ , a contradiction. So  $n(9, 176) \geq 355$ . By Table 4.1,  $n(9, 176) \leq 355$ . Therefore  $n(9, 176) = 355$ .



## CHAPTER V

### OPTIMUM CODES OF DIMENSION 3 AND 4 OVER GF(4)

In [12] Dodunekov has shown that codes of dimension 1 and 2 meet the Griesmer bound. He also showed that a code of dimension 3 need not meet the Griesmer bound. The values of  $n_4(3,d)$  and bounds on  $n_4(4,d)$  are derived in this chapter by proving some general results.

#### V.A. GENERAL RESULTS

Let  $C$  be an  $[n, k, d]$  code and let  $x \in C$  with  $\text{wt}(x) = w$ . If  $w < d + \lceil w/q \rceil$  then  $\text{res}(C, x)$  is an  $[n-w, k-1, d_0]$ ,  $d_0 \geq d-w + \lceil w/q \rceil$  code. So  $n-w \geq k-1$  or  $w \leq n-k+1$ . This observation is useful in determining weight distribution of certain codes (Theorem 5.3) and is listed below as a lemma.

**Lemma 5.1.** If  $C$  is an  $[n, k, d]$  code having a vector of weight  $w$ ,  $w < d + \lceil w/q \rceil$  then  $w \leq n-k+1$ .

Proposition 2.8, proved by Dodunekov and Manev [16] can be generalized for codes over GF( $q$ ).

**Theorem 5.1.** Let  $d \leq q^k$  and let  $n_q(k, d) \geq g_q(k, d) + t$ , for some positive integer  $t$ . Then  $n_q(k+1, d) \geq g_q(k+1, d) + t$ .

**Proof.** For  $d \leq q^k$ ,  $g_q(k+1, d) = g_q(k, d) + 1$ . Hence  $n_q(k+1, d) \geq n_q(k, d) + 1 \geq g_q(k, d) + t + 1 = g_q(k+1, d) + t$ .

A relation between codes over  $GF(p^m)$  and codes over  $GF(p^s)$ ,  $s$  a divisor of  $m$ , is given by the following theorem.

**Theorem 5.2.** Let  $C$  be an  $[n, k, d]$  code over  $GF(p^m)$  and let  $s$  be a positive divisor of  $m$ . Then there exists an  $[n(p^m-1)/(p^s-1), tk, (p^s)^{t-1}d]$  code over  $GF(p^s)$ ,  $t = m/s$ .

**Proof.** Let  $n' = (p^m-1)/(p^s-1)$ . Note that  $n'$  is the length of the Simplex code  $S_t(p^s)$  and  $t$  is the dimension of the vector space  $GF(p^m)$  over the field  $GF(p^s)$ . Let  $\{\alpha_1, \alpha_2, \dots, \alpha_t\}$  be a basis for  $GF(p^m)$  and let  $\beta_1, \beta_2, \dots, \beta_t$  be the rows of a generator matrix of  $S_t(p^s)$ . Then the linear mapping  $f$  from  $GF(p^m)$  into  $GF(p^s)^{n'}$  satisfying  $f(\alpha_i) = \beta_i$  is an isomorphism. Mapping each codeword  $(x_1, x_2, \dots, x_n) \in C$  to  $(f(x_1), f(x_2), \dots, f(x_n))$  one gets an  $[n(p^m-1)/(p^s-1), tk, (p^s)^{t-1}d]$  code over  $GF(p^s)$ .

The above theorem proves useful in (i) showing nonexistence of certain codes over  $GF(p^m)$  (ii) the construction of codes over  $GF(p^m)$ . This will be demonstrated in Sections V.C, V.D.

#### V.B. DETERMINATION OF $n_4(3, d)$

Let  $C$  be an  $[n_4(3, d), 3, d]$  code over  $GF(4)$ . By (2.11) and (2.12) it is easy to see that  $C$  meets the Griesmer bound for all  $d$  except for  $d = 7$  and  $8$ . The following theorem shows that  $n_4(3, 7) > g_4(3, 7)$ .

**Theorem 5.3.** There does not exist a  $[10,3,7]$  code over  $GF(4)$ .

**Proof.** Suppose there exists a  $[10,3,7]$  code  $C$  over  $GF(4)$ . Then  $A_0 = B_0 = 1$  and  $B_1 = 0$ . By Lemma 5.1  $A_9 = 0$ . So possible nonzero weights in  $C$  are 7, 8 and 10. MacWilliams equations [38] for  $B_0$  and  $B_1$  are

$$A_7 + A_8 + A_{10} = 63 \quad \text{and} \quad 3A_7 + 2A_8 = 150$$

respectively. Let  $c_1$  and  $c_2$  be any two codewords of weight 10. Then  $c_1$  and  $c_2$  are linearly dependent. For, if they are linearly independent, then by Lemma 2.13(i) of [29]  $wt(c_1) + wt(c_2) \leq 19$ , a contradiction. Therefore if  $A_{10} \neq 0$  then  $A_{10} = 3$  and hence  $A_7 = A_8 = 30$ , but then the MacWilliams equation for  $B_2$  gives  $B_2 = -15/4$ , a contradiction. So  $A_{10} = 0$  and one gets  $A_7 = 24$ ,  $A_8 = 39$  and  $B_2 = -6$ , a contradiction.

**Corollary 5.1.**  $n_4(3,7) = 11$  and  $n_4(3,8) = 12$ .

**Proof.** By Proposition 2.14 and Theorem 5.3,  $n_4(3,8) \geq 12$ . Let  $C$  be a  $[15,6,8]$  code over  $GF(4)$  [10]. Since  $15 = g_4(6,8)$  by Theorem 5.1,  $n_4(3,8) \leq g_4(3,8)+1 = 12$  and hence  $n_4(3,8) = 12$ . Deleting any coordinate of a  $[12,3,8]$  code over  $GF(4)$ , one gets an  $[11,3,7]$  code over  $GF(4)$ . So  $n_4(3,7) \leq 11$ . Hence by Theorem 5.3  $n_4(3,7) = 11$ .

# V.C. BOUNDS ON $n_4(4,d)$

**Theorem 5.4.** If  $k \geq 4$  and  $d \in \{4^{k-2}-1, 4^{k-2}, 2 \cdot 4^{k-2}-5, 2 \cdot 4^{k-2}-4, 3 \cdot 4^{k-2}-5, 3 \cdot 4^{k-2}-4\}$  then  $n_4(k,d) > g_4(k,d)$ .

**Proof.** In view of Proposition 2.14 one needs to prove the inequality ' $n_4(k,d) > g_4(k,d)$ ' for  $d = 4^{k-2}-1, 2 \cdot 4^{k-2}-5$ , and  $3 \cdot 4^{k-2}-5$  only. Let  $d = 4^{k-2}-1$  and let  $C$  be a  $[g_4(k,d), k, d]$  code over  $GF(4)$ . By Theorem 5.2 there exists a  $[2^{2k-2}-1, 2k, 2^{2k-2}-1]$  code  $C'$  over  $GF(2)$ . But a binary code with these parameters does not exist as  $n(2k, 2^{2k-2}-2) = 2^{2k-2}-2$  and  $n(k, 2^{k-3}-2) \geq g(k, 2^{k-3}-2)$  for  $k \geq 7$  (Proposition 2.9).

If  $d = 2 \cdot 4^{k-2}-5$  and if  $C$  is a  $[g_4(k,d), k, d]$  code over  $GF(4)$  then by Theorem 5.2 there exists a  $[2^{2k-1}-17, 2k, 2^{2k-2}-10]$  binary code  $C'$  and hence  $\text{res}(C', 2^{2k-2}-10)$  is a  $[(n(2k-1, 2^{2k-3}-5) + 1), 2k-1, 2^{2k-3}-5]$  code which does not exist for  $k \geq 5$  [17; Lemma 4.2]. Also  $\text{res}(C', 2^{2k-2}-10)$  code does not exist for  $k = 4$  as  $n(7, 27) = g(7, 27) + 2$  [43].

Finally, if  $d = 3 \cdot 4^{k-2}-5$  and if  $C$  is a  $[g_4(k,d), k, d]$  code over  $GF(4)$  then there exists a  $[3 \cdot 2^{2k-2}-18, 2k, 3 \cdot 2^{2k-3}-10]$  binary code  $C'$ . But a binary code with these parameters does not exist as  $g(2k, 3 \cdot 2^{2k-3}-10) = 3 \cdot 2^{2k-2}-18$  and  $n(k, 3 \cdot 2^{k-3}-10) \geq g(k, 3 \cdot 2^{k-3}-10) + 1$  for  $k \geq 8$  (Proposition 2.3)

**Theorem 5.5.** If  $d \in \{3, 4, 7, 8, 15, 16, 43, 44\}$  or if  $25 \leq d \leq 32$  then  $n_4(4,d) > g_4(4,d)$ .

**Proof.** If  $d \in \{3, 4, 7, 8, 15, 16, 43, 44\}$  then the inequality  $n_4(4,d) > g_4(4,d)$  follows using Proposition 2.13 (for  $d = 3, 4$ ),

Corollary 5.1, Theorem 5.1 (for  $d = 7, 8$ ) and Theorem 5.4 (for  $d = 15, 16, 43, 44$ ). If a  $[g_4(4, d), 4, d]$  code  $C$  over  $GF(4)$  exists for  $25 \leq d \leq 28$  ( $29 \leq d \leq 32$ ) then  $\text{res}(C, d)$  is a  $[10, 3, 7]$  ( $[11, 3, 8]$ ) code, a contradiction.

Putting  $q = 4$  and  $k = 4$  in Proposition 2.12 one gets the following theorem.

**Theorem 5.6.**  $n_4(4, d) = g_4(4, d)$  for  $45 \leq d \leq 48$ ,  $57 \leq d \leq 64$ ,  $93 \leq d \leq 96$ ,  $105 \leq d \leq 112$ ,  $117 \leq d \leq 128$ ,  $141 \leq d \leq 144$ ,  $157 \leq d \leq 160$ ,  $173 \leq d \leq 192$ ,  $201 \leq d \leq 208$  and  $d \geq 213$ . Moreover if the equality ' $n_4(4, d) = g_4(4, d)$ ' holds for  $d = 33 + t_1$ ,  $0 \leq t_1 \leq 7$  ( $d = 9 + t_2$ ,  $0 \leq t_2 \leq 15$ ) then it also holds for  $d = 161 + t_1(137 + t_2)$ .

Since codes of dimension 2 meet the Griesmer bound, there exists a  $[g_{16}(2, d), 2, d]$  code over  $GF(4)$ . Hence by Theorem 5.2 one gets the following result.

**Theorem 5.7.** There exists a  $[5g_{16}(2, d), 4, 4d]$  code over  $GF(4)$ .

**Corollary 5.2.** If  $49 \leq d \leq 56$  or  $113 \leq d \leq 116$ , then  $n_4(4, d) = g_4(4, d)$ . Moreover  $n_4(4, d) = g_4(4, d) + 1$  for  $d = 43, 44$ . **Proof.** If  $d = 52, 56$  or  $116$  then  $5g_{16}(2, d/4) = g_4(4, d)$ . Thus by Proposition 2.14,  $n_4(4, d) = g_4(4, d)$  for  $49 \leq d \leq 56$  and  $113 \leq d \leq 116$ . Moreover  $5g_{16}(2, 11) = g_4(4, 44) + 1$ . Deleting any coordinate of a  $[g_4(4, 44) + 1, 4, 44]$  code over  $GF(4)$  one gets a  $[g_4(4, 43) + 1, 4, 43]$  code over  $GF(4)$ .

Table 5.1 below gives the lower and upper bounds on  $n_4(4, d)$  for remaining values of  $d$ . The lower bounds are obtained by applying (2.2) and Theorem 5.5, while the upper bounds are obtained using Theorem 5.7.

Table 5.1

| d  | $n_4(4, d)$ | d   | $n_4(4, d)$ | d   | $n_4(4, d)$ |
|----|-------------|-----|-------------|-----|-------------|
| 3  | 7-9         | 67  | 91-94       | 136 | 182-185     |
| 4  | 8-10        | 68  | 92-95       | 137 | 184-187     |
| 5  | 9-12        | 69  | 94-97       | 138 | 185-188     |
| 6  | 10-13       | 70  | 95-98       | 139 | 186-189     |
| 7  | 12-14       | 71  | 96-99       | 140 | 187-190     |
| 8  | 13-15       | 72  | 97-100      | 145 | 195-197     |
| 9  | 14-17       | 73  | 99-102      | 146 | 196-198     |
| 10 | 15-18       | 74  | 100-103     | 147 | 197-199     |
| 11 | 16-19       | 75  | 101-104     | 148 | 198-200     |
| 12 | 17-20       | 76  | 102-105     | 149 | 200-202     |
| 13 | 19-22       | 77  | 104-107     | 150 | 201-203     |
| 14 | 20-23       | 78  | 105-108     | 151 | 202-204     |
| 15 | 22-24       | 79  | 106-109     | 152 | 203-205     |
| 16 | 23-25       | 80  | 107-110     | 153 | 205-207     |
| 17 | 25-27       | 81  | 110-112     | 154 | 206-208     |
| 18 | 26-28       | 82  | 111-113     | 155 | 207-209     |
| 19 | 27-29       | 83  | 112-114     | 156 | 208-210     |
| 20 | 28-30       | 84  | 113-115     | 161 | 216-217     |
| 21 | 30-32       | 85  | 115-117     | 162 | 217-218     |
| 22 | 31-33       | 86  | 116-118     | 163 | 218-219     |
| 23 | 32-34       | 87  | 117-119     | 164 | 219-220     |
| 24 | 33-35       | 88  | 118-120     | 165 | 221-222     |
| 25 | 35-37       | 89  | 120-122     | 166 | 222-223     |
| 26 | 36-38       | 90  | 121-123     | 167 | 223-224     |
| 27 | 38-39       | 91  | 122-124     | 168 | 224-225     |
| 28 | 39-40       | 92  | 123-125     | 169 | 226-227     |
| 29 | 41-42       | 97  | 131-132     | 170 | 227-228     |
| 30 | 42-43       | 98  | 132-133     | 171 | 228-229     |
| 31 | 43-44       | 99  | 133-134     | 172 | 229-230     |
| 32 | 44-45       | 100 | 134-135     | 193 | 259-262     |
| 33 | 46-47       | 101 | 136-137     | 194 | 260-263     |
| 34 | 47-48       | 102 | 137-138     | 195 | 261-264     |
| 35 | 48-49       | 103 | 138-139     | 196 | 262-265     |
| 36 | 49-50       | 104 | 139-140     | 197 | 264-267     |
| 37 | 51-52       | 129 | 174-177     | 198 | 265-268     |
| 38 | 52-53       | 130 | 175-178     | 199 | 266-269     |
| 39 | 53-54       | 131 | 176-179     | 200 | 267-270     |
| 40 | 54-55       | 132 | 177-180     | 209 | 280-282     |
| 41 | 56-57       | 133 | 179-182     | 210 | 281-283     |
| 42 | 57-58       | 134 | 180-183     | 211 | 282-284     |
| 65 | 89-92       | 135 | 181-184     | 212 | 283-285     |
| 66 | 90-93       |     |             |     |             |

## V.D. SOME IMPROVEMENTS IN TABLE 5.1

The 4x8 matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

generates an  $[8,4,4]$  code over  $GF(4)$ . By deleting any column of  $G$  one gets a  $[7,4,3]$  code over  $GF(4)$ . Thus

**Theorem 5.8.**  $n_4(4,3) = 7$  and  $n_4(4,4) = 8$ .

**Theorem 5.9.**  $n_4(4,5) = 9-10$ ,  $n_4(4,6) = 10-11$ ,  $n_4(4,7) = 12$  and  $n_4(4,8) = 13$ .

**Proof.** Let  $C$  be a  $[15,6,8]$  code over  $GF(4)$  [10]. By Table 5.1  $13 \leq n_4(4,8) \leq 15$  and by Theorem 5.1  $n_4(4,8) \leq 13$ . Hence  $n_4(4,8) = 13$ . By successively deleting a coordinate of a  $[13,4,8]$  code over  $GF(4)$  one gets  $[12,4,7]$ ,  $[11,4,6]$  and  $[10,4,5]$  codes over  $GF(4)$ .

If  $C$  is a  $[51,8,24]$  code, then Dodunekov and Manev [16] have shown that  $C$  has a generator matrix  $G$  whose columns with numbers  $\{i, i+17, i+34\}$  add upto zero for  $1 \leq i \leq 17$ . Let  $G_1$  be the matrix obtained from  $G$  by permuting columns so that its columns with numbers  $\{3i-2, 3i-1, 3i\}$  add upto zero for  $1 \leq i \leq 17$ . Any three columns of  $G_1$  with numbers  $\{3i-2, 3i-1, 3i\}$  ;  $1 \leq i \leq 17$  have the rows  $ooo, oll, lol$  or  $llo$ . If  $\omega$  is a primitive element of  $GF(4)$ , replacing  $ooo$

by 0,011 by 1,101 by  $\omega$  and 110 by  $\omega^2$  in  $G_1$ , one gets a  $[17,4,12]$  code  $C'$  over  $GF(4)$ . By successively deleting a coordinate of  $C'$ , the following theorem is obtained.

**Theorem 5.10.**  $n_4(4,12-j) = 17-j$  for  $0 \leq j \leq 3$ .

Applying the above procedure to the  $8 \times 60$  binary matrix

$$G_2 = \left[ \begin{array}{c|cccccccccccc} G_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{array} \right],$$

where  $G_1$  is as defined in the proof of Theorem 5.10, one gets a  $[20,4,13]$  code over  $GF(4)$ . Thus

**Theorem 5.11.**  $n_4(4,13) \leq 20$ .

**Theorem 5.12.**  $n_4(4,16-j) \leq 24-j$ ,  $0 \leq j \leq 2$ .

**Proof.**  $S_3(4)$  is a  $[21,3,16]$  code over  $GF(4)$ . By Theorem 3.27  $R(S_3(4)) = 13+t$ ,  $t \geq 0$ . So there exists  $x \in GF(4)^{21}$  with  $d(x, S_3(4)) = 13+t$  and the matrix

$$\left[ \begin{array}{c|ccc} x & 1 & 1 & 1 \\ \hline G_3(4) & 0 & & \end{array} \right]$$

generates a  $[24,4,16]$  code  $C$  over  $GF(4)$ . By successively deleting coordinates of  $C$  one gets  $[24-j,4,16-j]$  codes over  $GF(4)$  for  $0 \leq j \leq 2$ .



Using Theorems 5.6 and 5.10, existence of certain Griesmer codes over  $GF(4)$  is proved.

**Theorem 5.13.** If  $137 \leq d \leq 140$  then any  $[n_4(4,d), 4, d]$  code over  $GF(4)$  is a Griesmer code.

Successively deleting coordinates of a  $[g_4(4,137), 4, 137]$  code over  $GF(4)$  one gets the following result.

**Theorem 5.14.** (i) If  $133 \leq d \leq 136$ , then  $n_4(4,d) \leq g_4(4,d)+1$ .  
(ii) If  $129 \leq d \leq 132$ , then  $n_4(4,d) \leq g_4(4,d)+2$ .

A summary of new bounds derived in Theorems 5.8-5.14 is given by the following table.

Table 5.2

| d  | $n_4(4,d)$ | d   | $n_4(4,d)$ | d   | $n_4(4,d)$ |
|----|------------|-----|------------|-----|------------|
| 3  | 7          | 12  | 17         | 133 | 179-180    |
| 4  | 8          | 13  | 19-20      | 134 | 180-181    |
| 5  | 9-10       | 14  | 20-22      | 135 | 181-182    |
| 6  | 10-11      | 15  | 22-23      | 136 | 182-183    |
| 7  | 12         | 16  | 23-24      | 137 | 184        |
| 8  | 13         | 129 | 174-176    | 138 | 185        |
| 9  | 14         | 130 | 175-177    | 139 | 186        |
| 10 | 15         | 131 | 176-178    | 140 | 187        |
| 11 | 16         | 132 | 177-179    |     |            |

## REFERENCES

- [1] M.J. Adams, "'Subcodes and Covering Radius'", IEEE Trans. Inform. Theory, Vol. IT-32, pp. 700-701, 1986.
- [2] L.D. Baumert and R.J. McEliece, "'A note on the Griesmer bound'", IEEE Trans. Inform. Theory, Vol. IT-19, pp. 134-135, 1973.
- [3] B.I. Belov, "'A conjecture on the Griesmer bound'", Optimization Methods and Their Applications, All-Union Summer Sem., Lake Baikal, 1972.
- [4] B.I. Belov, V.N. Logachev and V.P. Sandimirov, "'Construction of a class of linear binary codes achieving the Varshamov-Griesmer bound'", Prob. Inform. Transm., Vol. 10, pp. 211-217, 1974.
- [5] E. Berlekamp and L.R. Welch, "'Weight distributions of the cosets of the (32,6) Reed-Muller code'", IEEE Trans. Inform. Theory, Vol. IT-18, pp. 203-207, 1972.
- [6] R.C. Bose, "'Mathematical theory of the symmetrical factorial design, 'Sankhya, Vol. 8, pp. 107-166, 1947.
- [7] P.B. Busschbach, M.G.L. Gerretzen and H.C.A van Tilborg, "'On the covering radius of binary, linear codes meeting the Griesmer bound'", IEEE Trans. Inform. Theory, Vol. IT-31, pp. 465-468, 1985.
- [8] G.D. Cohen, M.R. Karpovsky, H.F. Mattson Jr. and J.R. Schatz, "'Covering radius-Survey and recent results IEEE Trans. Inform. Theory, Vol. IT-31, pp. 328-343, 1985
- [9] G.D. Cohen, A.C. Lobstein and N.J.A. Sloane, "'Further results on the covering radius of codes'", IEEE Trans. Inform. Theory, Vol. IT-32, pp. 680-694, 1986.
- [10] J.H. Conway, S.J. Lomonaco Jr. and N.J.A. Sloane, "'A [45,13] code with minimum distance 16'", Preprint.
- [11] P. Delsarte, "'Four fundamental parameters of a code and their combinatorial significance'", Information and Control, Vol. 23, pp. 407-438, 1973.
- [12] S.M. Dodunekov, "'Minimal block length of a linear q-ary code with specified dimension and code distance'", Prob. Inform. Transm., Vol. 20, pp. 239-249, 1984.
- [13] S.M. Dodunekov, Proceedings of the fourth joint Swedish-Soviet International workshop in Information Theory, 27 Aug. to 1 Sep. 1989, Gotland, Sweden.

- [14] S.M. Dodunekov, T. Helleseeth, N.L. Manev and Ø. Ytrehu  
'New bounds on binary linear codes of dimension eight  
IEEE. Trans. Inform. Theory, Vol. IT-33, pp. 917-919,1
- [15] S.M. Dodunekov and N.L. Manev, 'Minimal possible bloc  
length of a linear binary code for some distances'',  
Prob. Inform. Transm., Vol. 20, pp. 8-14,1984.
- [16] S.M. Dodunekov and N.L. Manev, 'An improvement of  
the Griesmer bound for some small minimum distances'',  
Discrete Applied Mathematics, Vol. 12, pp. 103-114,198
- [17] S.M. Dodunekov and N.L. Manev, 'An improvement of  
the Griesmer bound for some classes of distances'',  
Prob. Inform. Transm., Vol. 23, pp. 38-46,1987.
- [18] D.E. Downey and N.J.A. Sloane, 'The covering radius  
of cyclic codes of length upto 31'', IEEE Trans.  
Inform. Theory, Vol. IT-31, pp. 446-447,1985.
- [19] P.G. Farrell, 'Linear binary anticode', 'Electronics  
Letters, Vol. 6, pp. 419-421, 1970.
- [20] R.A. Games, 'The packing problem for projective  
geometries over GF(3) with dimension greater than five  
Journal of Combinatorial Theory, Ser.A, Vol. 35,  
pp. 126-144,1983.
- [21] R.L. Graham and N.J.A. Sloane, 'On the covering  
radius of codes'', IEEE Trans. Inform. Theory, Vol. IT  
pp. 385-401,1985.
- [22] J.H. Griesmer, 'A bound for error-correcting codes'',  
IBMJ. Res. Develop., Vol. 4, pp. 532-542,1960.
- [23] T. Helleseeth, 'A characterization of codes meeting  
the Griesmer bound'', Information and Control. Vol. 50  
pp. 128-159,1981.
- [24] T. Helleseeth, New constructions of codes meeting  
the Griesmer bound'', IEEE Trans. Inform. Theory,  
Vol. IT-29, pp. 434-439,1983.
- [25] T. Helleseeth, T. Kløve and J. Mykkeltviet, 'On the  
covering radius of binary codes'', IEEE Trans. Inform.  
Theory, Vol. IT-24, pp. 627-628,1978.
- [26] T. Helleseeth and H.C.A. van Tilborg, 'A new class of  
codes meeting the Griesmer bound'', IEEE Trans. Inform  
Theory, Vol. IT-27, pp. 548-555,1981.
- [27] T. Helleseeth and Ø.Ytrehus, 'New bounds on the  
minimum length of binary linear block codes of dimensi  
8'', Reports in Informatics, Department of Informatics  
University of Bergen, Norway, Report No. 21,1986.

- [28] R. Hill, A first course in coding theory, Clarendon, Oxford, 1986.
- [29] R. Hill, Some optimal ternary linear codes'', Ars Combinatoria, Vol. 25A, pp. 61-72, June 1988.
- [30] J.W.P. Hirschfeld, ''Maximum sets in finite projective spaces'', Surveys in Combinatorics, LMS Lecture Note Series 82, pp. 55-76, 1983.
- [31] H. Janwa, ''Relations among parameters of codes'', Ph.D. Thesis, Syracuse University, U.S.A., 1986.
- [32] H. Janwa, ''Some new upper bounds on the covering radius of binary linear codes'', IEEE Trans. Inform. Theory, Vol. IT-35, pp. 110-122, 1989.
- [33] H. Janwa, ''Some optimal codes from algebraic geometry and their covering radii'', Presented at IMA Conference, June 1988, to appear in European Journal of Combinatorics.
- [34] H. Janwa, ''On the covering radius of  $q$ -ary codes'', to appear.
- [35] K.E. Kilby and N.J.A. Sloane, ''On the covering radius problem for codes I and II'', Siam Journal Alg. Disc. Meth., Vol. 8, pp. 604-627, 1987.
- [36] V.W. Logacev, ''An improvement of Griesmer bound in the case of small code distance, ''Optimization Methods and their Applications, All-Union Summer Sem., Lake Baikal, pp. 107-111, 1972.
- [37] V.N. Logachev, ''Characterization and existence conditions of codes meeting the Varshamov-Griesmer bound'', Proble Peredachi Informatsii, Vol. 24, pp. 24-41, 1988.
- [38] F.J. MacWilliams and N.J.A. Sloane, The theory of error correcting codes, North Holland, Amsterdam, 1981.
- [39] H.F. Mattson Jr., ''An improved upper bound on covering radius'', Lecture Notes in Computer Science, 228, New York: Springer-Verlag, pp. 90-106, 1986.
- [40] J. Mykkeltviet, ''The covering radius of the  $(128, 8)$  Reed-Muller code is 56'', IEEE Trans. Inform. Theory, Vol. IT-26, pp. 359-362, 1980.
- [41] G. Solomon and J.J. Stiffler, ''Algebraically punctured cyclic codes'', Information and Control, Vol. 8, pp. 170-179, 1965.

- [42] H.C.A. van Tilborg, ''On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound'', Information and Control, Vol. 44, pp. 16-35, 198
- [43] H.C.A. van Tilborg, ''The smallest length of binary 7-dimensional linear codes with prescribed minimum distance'', Discrete Mathematics, Vol. 33, pp. 197-207, 19
- [44] T. Verhoeff, ''An updated table of minimum-distance bounds for binary linear codes'', IEEE Trans. Inform. Theory, Vol. IT-33, pp. 665-680, 1987.

140.84

74  
519.44  
6101.0

### Date Slip

This book is to be returned on the  
date last stamped.

MATH-1990-D-GAR-0PT